UNIVERSIDADE FEDERAL DE SANTA CATARINA — UFSC
CENTRO DE CIÊNCIAS JURÍDICAS — CCJ
CURSO DE GRADUAÇÃO EM DIREITO

RAFAEL DE SOUZA

A TROCA DA SEGURANÇA PELA LIBERDADE NA INTERNET: UMA ANÁLISE DAS CONSEQUÊNCIAS DO COMÉRCIO ELETRÔNICO.

Florianópolis
2018

RAFAEL DE SOUZA

A TROCA DA SEGURANÇA PELA LIBERDADE NA INTERNET: UMA ANÁLISE DAS CONSEQUÊNCIAS DO COMÉRCIO ELETRÔNICO.

Trabalho de Conclusão de Curso submetido à banca examinadora da Universidade Federal de Santa Catarina- UFSC, como requisito parcial à obtenção do título de Bacharel em Direito.

Orientador: Professor Dr. Aires José Rover

Florianópolis
2018

UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS JURÍDICAS
COLEGIADO DO CURSO DE GRADUAÇÃO EM DIREITO

TERMO DE APROVAÇÃO

O presente Trabalho de Conclusão de Curso, intitulado "**A troca da segurança pela liberdade na internet: uma análise das consequências do comércio eletrônico**", elaborado pelo(a) acadêmico(a) **Rafael de Souza**, defendido em **27/11/2018** e aprovado pela Banca Examinadora composta pelos membros abaixo assinados, obteve aprovação com nota 9,5 (nove, cinco) cumprindo o requisito legal previsto no art. 10 da Resolução nº 09/2004/CES/CNE, regulamentado pela Universidade Federal de Santa Catarina, através da Resolução nº 01/CCGD/CCJ/2014.

Florianópolis, 27 de Novembro de 2018.

Aires José Rover
Professor Orientador

Egon Bockmann Wald Junior
Membro de Banca

Maurício José Ribeiro Rotta
Membro de Banca

Universidade Federal de Santa Catarina

Centro de Ciências Jurídicas

COORDENADORIA DO CURSO DE DIREITO

TERMO DE RESPONSABILIDADE PELO INEDITISMO DO TCC E ORIENTAÇÃO IDEOLÓGICA

Aluno(a): **Rafael de Souza**
RG: 096.291.159-30
CPF: 5.835.872
Matrícula: **14100233**
Título do TCC: **A troca da segurança pela liberdade na internet: uma análise das consequências do comércio eletrônico**
Orientador(a): **Aires José Rover**

Eu, **Rafael de Souza**, acima qualificado(a); venho, pelo presente termo, assumir integral responsabilidade pela originalidade e conteúdo ideológico apresentado no TCC de minha autoria, acima referido

Florianópolis, 27 de Novembro de 2018

Rafael de Souza
Rafael de Souza

AGRADECIMENTOS

Gostaria de agradecer aos meus familiares por todo o apoio prestado não somente durante minha jornada acadêmica, mas em toda minha vida. Por todos os conselhos, sermões, momentos felizes, cobranças, investimentos, amor e carinho durante todos esses anos. Em especial, aos meus avós, seu Aldo e dona Norma, e minha mãe, Aldanei, que desde meu nascimento me acolheram e me deram, com muito amor e dedicação, todo o necessário para até aqui chegar, me incentivando a sempre buscar o melhor para meu futuro.

A minhas tias, Aldaléa, por ser uma inspiração e exemplo de pessoa e profissional que um dia quero ser, e Aldanéa por todo o zelo e cuidado comigo.

A minha namorada, Victória Wall, por toda a parceria durante todos os anos em que estamos juntos, por todos os momentos felizes que compartilhamos e toda sua dedicação em sempre me ajudar.

A todos os meus professores, que contribuíram com minha formação, passando o conhecimento que um dia lhes fora passado, deixo aqui meu muito obrigado.

Ao professor Dr. Aires J. Rover, meu orientador, que me auxiliou na elaboração e conclusão desta monografia, sendo fundamental para que esta deixasse de ser uma ideia e se concretizasse.

A esta instituição de ensino, Universidade Federal de Santa Catarina, que a muito tempo, desde meu ensino fundamental, vem sendo minha segunda casa, e me proporcionando um crescimento pessoal e intelectual.

Agradeço também, a todos que de alguma forma tiveram alguma contribuição em minha trajetória.

Muito obrigado.

RESUMO

A presente monografia tem o objetivo de realizar um estudo da evolução do comércio eletrônico, demonstrado seus avanços, vantagens e desvantagens aos consumidores, comparando-a com o atual estado crescente tanto do próprio comércio, como do número de fraudes nele presentes. No primeiro capítulo, apresenta-se os conceitos básicos inerentes a este trabalho, como, de comércio eletrônico, crimes eletrônicos, liberdade e segurança. No segundo capítulo, analisa-se o atual aumento exponencial que vem acontecendo sobre o comércio eletrônico, e sobre o número de conflitos que surgem neste meio, de forma a apresentar dados estatísticos que fundamentem a proposta de intervenção. No terceiro capítulo, discute-se sobre esta proposta de intervenção, através da análise dos dados estatísticos e do olhar do consumidor sobre os atuais mecanismos de segurança e riscos sob os quais estes consumidores estão expostos, além de, uma averiguação sobre a implementação de novos métodos de segurança voltados para este meio. Sendo possível concluir que se faz necessário o implemento e regularização da segurança, mesmo que este resulte numa diminuição da liberdade individual dos consumidores. O método de pesquisa utilizado foi o indutivo, através estudo de caso, consultando dados estatísticos; pesquisa bibliográfica; e uma pesquisa qualitativa através da aplicação de um questionário via formulário eletrônico.

Palavras-chave: Liberdade. Segurança. Comércio Eletrônico. Direito Eletrônico. Fraudes.

ABSTRACT

The present term paper have the intent to realize a historic study about the evolution of the electronic commerce, showing their advances, benefits and disadvantages to consumers, comparing it with the actual growing state involving the commerce and the numbers of frauds that happen inside it. In the first chapter, it is presented the basic concept inherent at this work, like, the electronic commerce, electronic crimes, liberty and security. In the second chapter, it is analyzed the actual exponential increase that involves the electronic commerce and the numbers of conflicts that arise in this area, in order to present staticals datas that fundament the intervention proposal. In the third chapter, it is discussed the intervention proposal, analyzing statisticals datas and a consumer's look about the actual security mechanisms, the risks that these consumers are exposed and a fact-finding about the implementation of new security methods in this area. In conclusion, it is necessary to implement and regularize the security, even if results in a decrease in the individual liberty involving the consumers. The research method used was the inductive, through a case study, consulting statistical data; bibliographic research; and a qualitative research through the application of a questionnaire by an electronic form.

Keywords: Liberty. Security. Electronic Commerce. Electronic Law. Frauds.

INTRODUÇÃO 7
1 REVISÃO BIBLIOGRÁFICA 10
1.1 O COMÉRCIO ELETRÔNICO 10
1.1.1 As vantagens do comércio eletrônico 13
1.1.2 Os tipos de comércio eletrônico 14
1.1.3 Os contratos no comércio eletrônico 15
1.2 CRIMES ELETRÔNICOS 15
1.2.1 Definição de crimes eletrônicos 15
1.2.2 Os tipos de fraude em comércio eletrônico 17
1.2.3 Resolução dos conflitos 22
1.3 A CORRELAÇÃO DE SEGURANÇA E LIBERDADE 26
1.3.1 Mecanismos de segurança no comércio eletrônico 28
1.3.2 Liberdade no comércio eletrônico 33
2 APRESENTAÇÃO E FUNDAMENTAÇÃO DA PROPOSTA 35
2.1 ESTUDO DE CASO: O CRESCENTE NÚMERO DE USUÁRIOS REALIZANDO COMPRAS POR INTERMÉDIO DA INTERNET 35
2.2 O AUMENTO DOS CONFLITOS NO COMÉRCIO ELETRÔNICO 39
2.3 O PERFIL DO ATUAL USUÁRIO DO COMÉRCIO ELETRÔNICO 40
2.4 A NECESSIDADE DE NOVOS MECANISMOS DE SEGURANÇA 42
2.5 PROPOSTA PARA A DIMINUIÇÃO NA INCIDÊNCIA DE FRAUDES NO COMÉRCIO ELETRÔNICO 425
2.5.1 Confirmação de compra via SMS 46
2.5.2 Uso de programas que evitem a conexão do usuário com outros dispositivos enquanto realiza a compra 48
3 VERIFICAÇÃO DA PROPOSTA **50**
CONCLUSÃO 55
REFERÊNCIAS 57
APÊNDICE 1 **66**

INTRODUÇÃO

Com o advento da internet, e posteriormente sua expansão e popularização, o mundo como um todo se adaptou de forma a incluí-la e utilizá-la para realizar desde atividades simples, como pesquisar o significado, até as mais complexas, como a realização de cursos de graduação à distância (EaD) (PEREIRA, 1999).

Com a prática do comércio não foi diferente, desde a primeira venda online, em 1994, o nomeado comércio eletrônico, assim como a internet, vem avançando continuamente, acompanhando os avanços tecnológicos, como o uso de smartphones (MACAREZ; LESLÉ, 2002).

Atualmente grande parte das transações comerciais são realizadas através da internet, o que torna este um tema muito importante a ser estudado, necessitando, à medida que se dá sua expansão, de novos mecanismos e ferramentas que garantam a segurança de seus usuários, assim como normas que possam lhes garantir uma maior segurança jurídica (MARQUES, 2004).

Porém, apesar de apresentar muitos aspectos positivos, como por exemplo, uma maior comodidade para o consumidor, maior variedade de opções de produtos e de formas de pagamento, menores custos, e também, a implementação de produtos não possíveis no comércio físico tradicional (e-books, serviços de streaming, músicas, filmes, etc.), o comércio eletrônico também apresenta um lado negativo, principalmente quando observamos o número crescente de delitos que são cometidos através deste meio (NASCIMENTO; SILVA; SANTOS, 2009).

Nesta monografia, serão tratados os aspectos do comércio eletrônico, tendo como foco o comércio entre empresas e consumidor final, fazendo desde uma explicação de seus conceitos, até o estudo e apresentação de dados relevantes que retratam como se encontra o comércio eletrônico na atualidade, quais suas vantagens e desvantagens. Com o objetivo de averiguar se o uso do comércio eletrônico acarretou numa troca da segurança pela liberdade nas relações de comércio, fazendo com que surjam mais conflitos jurídicos, pois nos últimos anos houve um aumento considerável no comércio eletrônico em território nacional o que ocasionou também, em um aumento de crimes neste meio.

Para isso, serão utilizados os conceitos de liberdade e segurança de Thomas Hobbes e Jean-Jacques Rousseau, aplicando-os ao comércio eletrônico e verificando

seus impactos na sociedade atual. Estudando as liberdades proporcionadas por esta forma de comércio, e também, a aplicação de medidas de segurança.

No primeiro capítulo será realizada uma revisão bibliográfica, de forma a apresentar e conceituar o comércio eletrônico, demonstrando seu surgimento, aspectos legais, e as diferentes classificações de comércio eletrônico; apresentar como são definidos os crimes virtuais e resolvidos os conflitos criados a partir do comércio eletrônico; demonstrar os conceitos de liberdade e segurança e sua correlação.

No segundo capítulo será apresentada e fundamentada uma proposta que venha a resolver o crescente número de fraudes no comércio eletrônico, através da análise de dados estatísticos que demonstrem os fatos afirmados, assim como, os riscos e mecanismos de segurança do comércio eletrônico.

Por fim, no terceiro capítulo, proceder-se-á a discussão e verificação da proposta, demonstrando a necessidade de se criar novos mecanismos de segurança, e a aplicabilidade e eficácia das medidas propostas nesta monografia.

Para a realização deste trabalho se utilizou uma teoria de base à partir da observação e análise sistêmica do tema e dos casos concretos, com uma visão de mundo de Thomas Hobbes e Jean-Jacques Rousseau, de que a liberdade individual está relacionada a segurança do coletivo, e que o aumento de uma se dá a partir do detrimento da outra. Desta forma, verificando se na sociedade atual o mesmo conceito continua sendo aplicado, e se no meio virtual, através do comércio eletrônico, a corrente busca por maior liberdade acarreta em uma insegurança para seus usuários, e assim, ocasionando em um problema para o direito.

O método de abordagem utilizado é o indutivo, onde, com o problema e a hipótese estabelecidos, se verificou a veracidade das hipóteses levantadas, através de análise de dados estatísticos, e a aplicação de formulários eletrônicos para uma pesquisa qualitativa.

O procedimento utilizado foi um Estudo de caso, que consistiu em análise estatística de dados, que foram obtidos através de consulta e pesquisa a fontes que fornecem e realizam estudos estatísticos sobre o comércio eletrônico; assim como uma Pesquisa Bibliográfica, com consulta em artigos publicados, monografias e também em livros que discorrem sobre os assuntos abordados neste trabalho.

E também, uma pesquisa qualitativa, através de um formulário eletrônico, na forma de questionário (Apêndice 1), o qual foi respondido por 200 participantes, que

visou obter dados mais específicos em relação ao tema abordado, por exemplo, se estes usuários utilizam mecanismos de segurança, qual a frequência que realizam compras, se já foram vítimas de fraudes, entre outras perguntas. Esse formulário foi divulgado em redes sociais, como *Whatsapp*[1] *e Facebook*[2]*,* sendo que as perguntas foram divididas em dois grupos. O primeiro com a finalidade de obter um perfil do cliente de comércio eletrônico, assim como seus conhecimentos sobre este tipo de comércio. Já o segundo, com perguntas mais direcionadas a saber quão abertos estes clientes estão a implementação de novas medidas que possam diminuir a incidência das fraudes em comércio eletrônico.

Por fim, uma pesquisa hermenêutica, para poder elaborar e fundamentar a proposta de intervenção, assim como analisar sua aplicação.

[1] Divulgado em grupos que continham grande número de pessoas, e de forma individual para contatos.
[2] Divulgado em páginas e grupos.

1 REVISÃO BIBLIOGRÁFICA

1.1 O COMÉRCIO ELETRÔNICO

O comércio eletrônico só se tornou possível com a consolidação da internet, a qual desde sua “criação”, passou por diversas etapas, desde o simples envio de e-mail com pouco êxito. Um setor desacreditado onde em 1977 o responsável da Digital Equipment Corporation não via “quaisquer razões para alguém querer um computador em sua casa”. (MARQUEZ; ANJOS; VAZ, 2002 p.5). Até que em 1989 com a invenção do WWW (*World Wide Web)*, e assim realizada a “democratização” da internet ocorreu seu momento decisivo, o qual foi confirmado nos anos seguintes com a fundação do *Yahoo.!, Internet Explorer* e *Netscape*, assim como, a primeira venda de um livro pela *Amazon.com* (MACAREZ; LESLÉ, 2002 p. 20-22).

Correia (1999), alegou que nos dez anos seguintes à publicação de sua pesquisa iria ocorrer um fenômeno de “desaparecimento” da internet, não referindo que esta deixaria de existir, mas que se tornaria tão comum e habitual, que viraria uma necessidade diária das pessoas, tal como a energia elétrica, e deste modo, passaria a se tornar invisível para nós. E assim como previsto, nos dias atuais a falta da internet ocasiona grande transtorno para o cotidiano pessoal, de modo que tudo que fazemos está vinculado à rede.

São duas as definições de comércio eletrônico, uma mais “fraca” e outra mais “forte”. A primeira consiste em uma definição mais geral, abrigando quaisquer sistemas tecnológicos que facilitem a atividade comercial por meio de mecanismos eletrônicos. E a segunda é uma definição mais restrita, que além dos requisitos da primeira, necessita que toda a transação seja efetuada por meio de mecanismos eletrônicos, tais como, pagamento e entrega do produto ou prestação do serviço adquirido (SILVA, et al., 2003. p.2).

Já Fagundes (2011) define o comércio eletrônico como:

> *Definimos comércio eletrônico como qualquer transação comercial que envolve a cadeia de valor dos processos de negócio através de um ambiente eletrônico, por exemplo, a Internet. As práticas de comércio eletrônico não vieram com a Internet.*
> *[...]*

> *o comércio eletrônico como conhecemos hoje iniciou no final da década de 1960, mas desde 1993, novas tecnologias, em constante evolução, permitem às empresas realizar funções de negócios eletrônicos (e-business) com maior eficiência, rapidez e menores custos do que jamais foi possível. Um empreendimento de sucesso é aquele que consegue utilizar a tecnologia existente, adequada aos consumidores do seu nicho de mercado. Isso implica em conhecer o comportamento dos consumidores, as tecnologias e o seu próprio negócio. Reforçando: comportamento, tecnologia e negócio.*

Desde sua fundação, o comércio eletrônico, pela sua natureza híbrida de tradição (o comércio) e inovação (o eletrônico) faz repensar muitos dos princípios e concepções do mundo dos contratos. Teorias pensadas para o mundo físico confrontam agora a virtualidade imaterial das novas tecnologias e da Internet. Os autores incluem aqui as questões relativas à admissibilidade de documentos e contratos eletrônicos, formação do contrato, momento da celebração e conclusão, cláusulas abusivas, identificação dos contratantes e autenticidade das suas declarações. Outros dos problemas relacionam-se com a lei e jurisdição aplicáveis, e a resolução extrajudicial de litígios (PEREIRA, 1999).

Num outro ponto de vista, a realidade dos sujeitos participantes no grande mercado virtual exige respostas eficazes, que pressupõem mas não esperam pelas discussões doutrinárias e soluções legais. Empresas e consumidores receiam sobretudo pela segurança e confidencialidade das transações. Na ordem do dia da discussão pública, e na agenda política de estados e governantes está a tributação das transações eletrônicas de bens e serviços, a responsabilidade civil por atos ilegais e lesivos, a necessidade e medida da cooperação internacional, a proteção dos dados pessoais, a privacidade, a proteção dos direitos intelectuais e a fiabilidade dos meios de pagamento (COUTO, 2004 p.35).

Quanto a celebração do contrato, essa se dá pela transmissão eletrônica de dados, não sendo a manifestação de vontade das partes de forma oral ou por documento escrito. Ocorrendo a oferta e aceitação entre os contraentes por meio do registro virtual (COELHO, 2000. p. 37).

Por não haver o contato físico entre as partes, acaba surgindo o problema da certeza da identidade dos contratantes, problema este que teve como solução apresentada a criação da assinatura eletrônica (RODRIGUES, 2001. p. 92). Porém,

esta assinatura resolve o problema de forma parcial, pois resolve apenas o problema quanto às relações contratuais entre a o adquirente e um adquirido de maior porte (lojas, sites de comércio, etc.), mas quando esta relação se dá entre dois civis, de menor expressão, a impessoalidade continua a ser um problema.

Mas o pior problema são os infratores, e no comércio eletrônico, os mais destacados seriam os *Carders,* que são especialistas em fraudes através de cartões de crédito, e os *Scammers*, que são os que se utilizam de mensagens enganosas, propagandas falsas levando o indivíduo a fornecer informações sigilosas ou instalar softwares de espionagem (spyware), e principalmente do *phishing*[3]. O Brasil, é um dos países onde ocorre a maior incidência de infrações pela Internet (VOLPI, 2006. p. 50-51).

O local de celebração do contrato é outro problema, pois é comum no comércio eletrônico, que o adquirente seja de um país e o proponente de outro. Desta forma a interpretação que se faz é a partir do Código Civil, em seu art. 435 *"Reputar-se-á celebrado o contrato no lugar em que foi proposto"*, ou seja, no lugar onde se localiza o proponente, sendo este submetido às legislações daquele local. Porém, podem as partes no contrato, definir o foro competente (SILVA NETO, 2008).

No Brasil, o comércio eletrônico é regulado pelo Decreto 7.962/2013, que tem o objetivo de garantir a segurança jurídica dos consumidores que utilizam a internet para realizar contratos de aquisição de bens ou serviços, regulando-o, e estabelecendo as obrigações para aqueles que desejam fornecer tais bens ou serviços para esta demanda da internet (LUDMER, 2017).

Conforme Antonio Rulli Neto, Marcelo Adelino Asamura Azevedo e Renato Asamura Azevedo (2012),

> O importante em todas as situações é permitir que o consumidor conheça as condições do negócio e do produto ou serviço, partindo-se, como já colocamos, da ideia de boa-fé e transparência. Na dúvida entre o que colocar, é preferível inserir todas as informações essenciais sobre o negócio, de forma clara e inteligível, evitando dúvidas ou contradições a partir das informações e permitindo que o consumidor tenha segurança em decidir. Com tantos produtos novos e tantas opções, é preciso que o consumidor consiga escolher

[3] *Phishing* é a prática de criar um *website* idêntico ao de uma loja no intuito de enganar ou ludibriar consumidor a fornecer suas informações sigilosas, como número do cartão de crédito e Cadastro de Pessoa Física (CPF), assim podendo se utilizar destes dados como bem entender.

> conscientemente, sem truques ou mecanismos que o confundam ou o enganem.

O comércio eletrônico é muito similar ao comércio físico tradicional quando comparamos seus conceitos, sendo entendidos como os negócios celebrados entre empresas e clientes para a compra e venda de produtos ou prestação de serviços, tendo como fator determinante, a celebração do negócio se dar através do meio eletrônico (MARQUES, 2004).

1.1.1 As vantagens do comércio eletrônico

Além de ser mais cômodo ao cliente, menores preços, e uma maior variedade de produtos disponíveis, outra vantagem do comércio eletrônico é o fato de poder facilmente ficar aberto 24h por dia, 365 dias ao ano, fatores estes, que impulsionam o mercado. Fora isto, existe o fato de poder proporcionar ao consumidor que mora demasiadamente distante dos polos comerciais uma facilidade para que compre os produtos que necessita, sem precisar se deslocar grandes distâncias, poupando assim, tempo e dinheiro para o consumidor s (NASCIMENTO; SILVA; SANTOS, 2009).

Além das vantagens para os consumidores, o comércio eletrônico também se mostra vantajoso para as empresas, conforme explica Albertin (2010), o comércio eletrônico causa um aumento da relação cliente-fornecedor além de melhor comunicação entre as partes; possibilita novos modelos de negociação, assim, podendo adaptar produtos antes não disponíveis ao mercado; novas oportunidades; mais agilidade nas negociações.

Outro ponto, é a não necessidade de um espaço físico, como seria necessário em uma loja física, assim como a mesma demanda de funcionários, o que faz o custo da empresa, e consequentemente, do produto ser menor. Desta forma, o comércio eletrônico acaba possibilitando que as empresas ofereçam menores preços, em relação ao das lojas físicas, sem ter prejuízos (DINIZ et al., 2011).

Porém, como em qualquer negócio, o comércio eletrônico também apresenta desvantagens, a exemplo, a entrega, pois diferente de uma loja física, onde na maioria dos casos, você já sai com o produto, no comércio eletrônico é necessário que você aguarde alguns dias até que seja efetuada a entrega, o que se torna um problema quando você tem uma necessidade do produto com urgência (GODOFREDO, 2012).

Para Pitwak e Ferreira (2009, apud, COELHO; OLIVEIRA; ALMÉRI, 2013),

> *Um dos maiores desafios do e-commerce é questão da segurança, pois ao realizar uma compra, o cliente precisa informar seus dados pessoais, números de cartões de crédito e até senhas, fazendo com que o cliente tenha medo de efetuar a compra pela internet, pois infelizmente existem muitos casos de golpes virtuais.*

1.1.2 Os tipos de comércio eletrônico

Dentre as classificações de comércio eletrônico, a que mais se destaca é que se utiliza da natureza das partes para fazê-la, desta forma, dividindo o comércio eletrônico em seis grupos, conforme retrata CROCCO et al. (2012), são eles:

B2B - business to business, são as transações, seja compra de produtos ou prestação de serviços, realizadas através da internet entre duas diferentes empresas.

B2C - business to consumer, são as transações realizadas entre uma empresa e um consumidor final, sendo este o tipo de transação mais comum dentro do comércio eletrônico.

C2C - consumer to consumer, onde o negócio é realizado entre os consumidores, é o tipo de negócio que geralmente é feito com intermédio de uma plataforma externa as duas partes, a exemplo, *Mercado Livre*, *OLX*, entre outras. Porém, pode ser também realizado de forma direta, sem o auxílio de tais plataformas.

G2C - government to consumer, aquelas entre os órgãos do governo e os consumidores finais.

B2G - business to government, transações que ocorrem entre empresas e órgão governamentais, sendo os principais exemplos, o fornecimento e as licitações realizados através da internet.

G2G - government to government, que são aqueles negócios entre dois departamentos ou órgãos governamentais.

Ressalta-se, que nos tipos onde “fornecedor” e “consumidor” são de naturezas diferentes (B2C, G2C e B2G), o caminho inverso também é possível, desta forma, sendo classificados como C2B (consumer to business); C2G (consumer to government); e G2B (government to business).

1.1.3 Os contratos no comércio eletrônico

Contratos eletrônicos são definidos com os contratos celebrados através da transmissão de dados pela rede, Internet, contendo os aspectos jurídicos do negócio celebrado, inclusive, os atos que antecedem e sucedem o respectivo contrato (AQUINO JÚNIOR, 2012).

Embora não celebrados da forma tradicional, e com maior complexidade, em função de um maior número de sujeitos atrelados a ele, e também, por ser um contrato mais célere que o tradicional, muitas vezes, sem o contato direto entre as partes, aplicam-se a ele as mesmas normas, sejam elas civis ou consumeristas (Código Civil ou Código do Consumidor), de mesma maneira que em que se aplicam aos contratos físicos, tendo em vista que ambos os contratos possuem semelhanças jurídicas, diferindo-se somente quanto ao meio através do qual são celebrados e quanto a possibilidade de desistência no comércio eletrônico (MARTINS, 2016).

No Brasil, exceto quando exigido de forma expressa por lei, a declaração de vontade independe de forma especial, ou seja, o documental digital é válido para a formalização do comércio eletrônico. Sendo assim, o contrato eletrônico possui as mesmas condições, quanto a suas exigências, que os contratos tradicionais, e desta forma, não pode-se recusá-lo pelo fato de se tratar de um documento digital (KLEE, 2014).

1.2 CRIMES ELETRÔNICOS

1.2.1 Definição de crimes eletrônicos

Adeneele Garcia Carneiro (2012), classifica os crimes virtuais em dois tipos[4], os próprios, que são aqueles onde é essencialmente necessário o uso do computador para que se cometa tal crime, sendo o computador objeto e meio para o crime e que atinjam diretamente o software ou hardware dele, podendo só ser concretizados pelo computador ou contra ele e seus periféricos. Exemplos destes crimes são a invasão de dispositivos para alteração ou transferência de dados não autorizados.

[4] A autora também difere quanto ao sujeito, em ativo e passivo.

Enquanto os impróprios, são aqueles que são realizados através do dispositivo de informática, porém, não necessariamente necessitam deste para ocorrer, podendo ser realizados sem o uso do dispositivo, ou seja, são crimes já tipificados que passam a ser praticados através dos meios de informática, alguns exemplos são os art. 155 (furto), art. 147 (ameaça) do Código Penal, e o art. 247 da Lei n° 8.069/90 (Estatuto da Criança e do Adolescente) que tipifica a pedofilia (CARNEIRO, 2012).

Já Guilherme Feliciano (2000), retrata os crimes eletrônicos como,

> *"Conheço por criminalidade informática o recente fenômeno histórico-sócio-cultural caracterizado pela elevada incidência de ilícitos penais (delitos, crimes e contravenções) que têm por objeto material ou meio de execução o objeto tecnológico informático (hardware, software, redes, etc.)."*

Por sua vez, Emanuel Alberto Sperandio Garcia Gimenes (2013) define-o como,

> *[...] o crime virtual é qualquer ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão em que um computador conectado à rede mundial de computadores (Internet) seja o instrumento ou o objeto do delito.*

Conforme a Lei nº 12.737/12, que se propunha a alterar o Código Penal, o Código Penal Militar e a Lei nº 7.716/89, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares praticadas contra sistemas informatizados e similares, a grande dificuldade na construção dos tipos relativos aos crimes informáticos repousa na intangibilidade do seu objeto. Daí alguns doutrinadores identificaram que, nos delitos praticados com o uso do sistema informático, se teria como bem jurídico a informação, a inviolabilidade de dados informáticos ou, até mesmo, a capacidade funcional dos sistemas informáticos (REIS, 2015. p. 133).

Quanto ao local do crime esse será qualquer ponto no mapa de nosso território, onde houver marcador apontando computador, seja ele dos criminosos, do provedor ou do usuário, pois conforme o Código Penal, em seu artigo 6º "*Considera-se praticado o crime no lugar em que ocorreu a ação ou a omissão, no todo ou em parte,*

bem como onde se produziu ou devia-se produzir o resultado". Ou seja, o lugar do crime, é qualquer um no qual se realizou qualquer ato do delito (CARICATTI, 2006. p. 67).

1.2.2 Os tipos de fraude em comércio eletrônico

Existem diversos mecanismos de fraude no comércio eletrônico, dentre eles, os mais comuns são o *phishing*, e o uso de malwares, que tem por finalidade, roubar os dados do cartão de crédito do usuário e depois utilizá-lo para realizar compras virtuais.

Phishing, conforme a Microsoft (2017), é uma prática através da qual o criminoso tenta "pescar", daí o nome *phishing* em analogia ao *fishing* que em inglês significa pescar, se utilizando de um site muito parecido com o de grandes empresas confiáveis do comércio eletrônico, e enviam e-mails para os usuários, com o falso link (URL[5]) para o site, contendo geralmente, anúncios de promoções, em que os usuários que não estiverem atentos, acabam por fornecer seus dados, e assim, tendo estes roubados.

Já os malwares, são os softwares maliciosos que tem por finalidade danificar o hardware, ou obter dados presentes neste, sendo eles, os spywares, os vírus, os trojans, os worms, os ransomwares, os rootkits e os adwares (AVAST, 2017).

Para estes tipos de fraudes, onde o que geralmente ocorre é a compra através dos dados de cartão de crédito obtidos, quando isto ocorre, podem os usuários que foram vítimas pedir o *chargeback*, que é um "estorno" do valor cobrado, motivado pelo não reconhecimento da pessoa de uma compra realizada em seu cartão e presente em sua fatura. São quatro os tipos de *chargeback* existentes (FERREIRA, 2016).

Fraude, que é a prática mais comum, quando através do roubo de dados alguém utiliza o cartão de outro para realizar compras;

Auto-fraude, quando a própria pessoa, com má-fé, solicita o reembolso do valor de uma compra que ela mesma realizou;

---

[5] URL é o endereço de um recurso disponível em uma rede, seja a rede internet ou intranet, e significa em inglês *Uniform Resource Locator*, e em português é conhecido por Localizador Padrão de Recursos. Ou seja, o endereço virtual de um site.

Fraude-amiga, quando alguém próximo a pessoa faz a compra, seja ela esposa, filhos, ou até mesmo um amigo próximo, e a pessoa não reconhecendo a compra, pede o seu estorno;

E por fim, o Desacordo comercial, que é quando o consumidor afirma que algo na compra não foi como o combinado, seja a natureza do produto, ou a não entrega do mesmo (FERREIRA, 2016).

Conforme Fidel Beraldi (2014),

> *A facilidade de acesso a cartões de crédito e o aumento da sua utilização têm atraído criminosos interessados em ganhos ilícitos originados de transações fraudulentas. Um dos maiores atrativos é o ganho de grandes quantias em dinheiro em um curto espaço de tempo sem exposição a grandes riscos. Isto porque raramente criminosos são descobertos e presos por um longo tempo na atual legislação brasileira para esse tipo de crime.*

Os crimes de fraude, utilizando o cartão de crédito, podem ser divididos quanto ao tipo em: Invasão de conta, Cartão perdido ou roubado, Falsificação, E-commerce/MOTO, Extravio, Roubo de identidade.

Invasão de Conta como deixa claro o nome, é o ato criminoso de realizar uma transação com dados de um cartão ou outras funções bancárias, através da invasão mediante uso de log-in, número de conta, e senhas da vítima, em contas de bancos ou sites que possuem cadastrados seus dados pessoais.

Cartão perdido ou roubado, é o tipo que necessita de uma ação física, além da virtual, onde o fraudador se utiliza de um cartão de crédito, o qual achou, furtou ou roubou, o qual não lhe pertence, para realizar uma compra virtual como se seu dono o fosse.

Falsificação, é a clonagem de um cartão, ou seja, cria-se um cartão falso contendo os dados de um cartão verdadeiro pertencente a terceiro, e com este cartão em mãos, os fraudadores realizam compras, saques, e outras práticas delituosas coma finalidade de obter uma vantagem econômica.

E-commerce / MOTO, é o tipo de fraude realizada através do meio virtual principalmente, conforme Fidel Beraldi (2014),

> *É um tipo de fraude realizada através da internet, telefone, fax ou por carta, onde não existe a presença física do cartão. Na maioria das*

> *vezes, para realizar esse tipo de fraude, os dados dos cartões foram obtidos fisicamente através da cópia da trilha magnética do cartão ou vazamento de informações de transações anteriores que foram armazenadas por estabelecimentos que atuam no comércio eletrônico.*

Extravio é a prática de desviar os cartões, no ato de entrega destes ao seu proprietário, ou seja, no envio do cartão, saindo do banco tendo como destinatário o seu dono, estes são furtados e entregues a terceiros, que realizam o seu uso fraudulentamente.

Roubo de identidade, é um ato praticado na maioria das vezes por grupos criminosos, onde, após furtar dados de terceiros, estes criam contas em agências bancárias, realizando o pedido de cartões de crédito que serão utilizados com a finalidade de cometer os delitos (BERALDI, 2014).

Abaixo explicaremos os tipos de malwares:

1.2.2.1 Spywares

Os spywares são os malwares que tem o objetivo de monitorar ou espiar, as atividades realizadas em um computador ou celular. Desta forma, são utilizados principalmente para roubar os dados pessoais dos usuários, através do monitoramento de teclas do computador (REALPROTECT, 2015). Conforme o Avast[6] explica,

> *Spyware é um tipo de malware que é difícil de se detectar. Ele coleta informações sobre seus hábitos online, histórico de navegação ou informações pessoais (como números de cartão de crédito), e geralmente usa a internet para passar estas informações a terceiros sem você saber. Keyloggers são um tipo de spyware que monitora as teclas do seu teclado.*

[6] Avast é uma empresa que atua na proteção contra malwares, sendo o seu antivírus, um dos mais famosos e utilizados atualmente.

1.2.2.2 Vírus de computador

Já os vírus, são programas, ou códigos, que tem por objetivo, danificar o hardware, tornando-o frágil e vulnerável, seja para novas infecções de outros malwares, ou para uma invasão de hacker. São facilmente espalhados, basta abrir um link infectado, e compartilhado por mensagem que você, caso não tenha um bom antivírus em seu aparelho, já está infectado (TORRES, 2018).

Já conforme a Norton (2018),

> *Em termos mais técnicos, um vírus de computador é um tipo de programa ou código malicioso criado para alterar a forma como um computador funciona e desenvolvido para se propagar de um computador para outro. Um vírus atua se inserindo ou se anexando a um programa ou documento legítimo, que tenha suporte para macros, a fim de executar o seu código. Durante esse processo, um vírus pode potencialmente causar efeitos inesperados ou prejudiciais, como danificar o software do sistema, corrompendo ou destruindo os dados.*

1.2.2.3 Trojans

Os trojans, popularmente conhecidos como “cavalo de tróia”, são um tipo de malware que vem escondido em um download, seja ele de games, filmes, músicas, entre outros, e que se infiltram em seu computador assim que você executa o arquivo infectado. É um malware muito malicioso, pois ele além de roubar os dados do usuário, torna o computador, ou qualquer outro aparelho que você utilize, mais lento por sobrecarga de processamento (AVAST, 2017).

1.2.2.4 Worms

Conforme a Panda Security (2018), os worms,

> *São programas que geram cópias de si próprios em diversos locais num computador infectado. O objetivo deste tipo de malware é por norma saturar os computadores e redes, impedindo o seu correto funcionamento. Ao contrário dos vírus, os worms não infectam arquivos. Exploram vulnerabilidades das aplicações e das redes de comunicações para se propagarem, e não necessitam de intervenção das vítimas para se executarem.*

O principal objetivo dos worms é se espalhar e infectar o maior número possível de dispositivos, para isso, eles se multiplicam criando diversas cópias de si mesmo e são enviados através de e-mail, mensagens de textos, ou outras formas de conexão entre usuários (PANDA SECURITY, 2018).

1.2.2.5 Ransomwares

São os softwares maliciosos criados para bloquear o acesso do usuário infectado a um sistema ou arquivo, ao qual, só será permitido o acesso caso este venha a pagar um valor estipulado pelo criador do malware, em outras palavras, trata-se de um sequestro de arquivo ou sistema que ocorre de forma virtual (ALECRIM, 2016).

Conforme a Avast (2018),

> *Ransomware (também conhecido como rogueware ou scareware) restringe o acesso ao sistema do seu computador e pede que um resgate seja pago para que a restrição seja removida. Os ataques de ransomware mais perigosos são causados pelos ransomwares WannaCry, Petya, Cerber, Cryptolocker e Locky.*

1.2.2.6 Rootkits

São programas destinados a garantir ao hacker acesso a seu computador, podendo este administrá-lo da forma que bem entender sem que você saiba, isso porque os rootkits possuem a capacidade de se esconder em seu sistema, evitando assim, que sejam facilmente detectados. Eles podem infectar seu sistema por diferentes formas, sendo a mais comum através da instalação de aplicações contendo-o (AVAST, 2018).

Conforme Kaspersky (2013),

> *A capacidade de se esconder permite que este tipo de malware permaneça no sistema da vítima por meses, às vezes até anos,*

> *deixando que um hacker use o computador para o que bem entender. Mesmo uma máquina que não contém informações valiosas, o que é pouco comum, pode ser útil para produzir bitcoins (moeda digital), enviar spam e participar de ataques DDoS. A funcionalidade rootkit permite que os hackers escondam suas atividades criminosas não apenas de ferramentas de monitoramento embutidas no OS, mas de sensores de antivírus também.*

1.2.2.7 Adwares

São os malwares de publicidade, desta forma, aqueles que podemos ver e perceber sem o auxílio de programas. Na maioria dos casos, os adwares não oferecem riscos ao dispositivo, apenas atrapalham seu uso com o bombardeio de propagandas, o que muitas vezes acaba por ser irritante. Porém, em alguns dos casos, podem invadir a configuração do sistema, e assim, sendo exploradas por agentes maliciosos (LEMONNIER, 2016).

Conforme Kaspersky (2018),

> *Adware é o nome que se dá a programas criados para exibir anúncios no computador, redirecionar suas pesquisas para sites de anunciantes e coletar seus dados para fins de marketing. Por exemplo, eles rastreiam o tipo de sites que você costuma acessar para exibir anúncios personalizados.*
> *O adware, que coleta dados com seu consentimento, não deve ser confundido com programas de spyware do tipo cavalo de Troia, que coletam informações sem a sua permissão. Se o adware não avisar que está coletando informações, será considerado malicioso.*

1.2.3 Resolução dos conflitos

A resolução de conflitos se dá principalmente através da aplicação do Código de Defesa do Consumidor (CDC), que foi promulgado pela Lei nº 8.078, de 11 de setembro de 1990, o qual é garantido pela CF em seu artigo 5ª, inc. XXXII, e que vem sendo modificado de forma a garantir uma melhor garantia de proteção do consumidor. (PACHECO, 2015. p.15) E também pela aplicação de Legislação

Específica, a exemplo a Lei nº 12.737, de 30 de novembro de 2012, ou "Lei Carolina Dieckmann"[7], que dispõe da tipificação criminal de delitos informáticos.

Com o advento do Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014, que discorre sobre os deveres e os direitos dos usuários e fornecedores de serviços dentro da rede mundial de computadores, Internet, regulamenta que a responsabilidade do provedor de conexão à internet se responsabiliza de duas formas: *primeira*, em respeito à liberdade de expressão, o provedor só se responsabiliza pelo conteúdo gerado por terceiros, se mediante decisão judicial, não retirar o conteúdo ou tomar as medidas sancionadas dentro do tempo estipulado. *Segunda:* nos casos onde houver *"conteúdos envolvendo cenas de nudez ou de sexo"* este deverá ser retirado logo após o pedido realizado pela vítima, para evitar que haja maiores prejuízos a esta (OLIVEIRA, 2014. p. 20).

Em Agosto de 2018, uma nova lei foi promulgada, com a finalidade de proteger os dados pessoais dos usuários da internet. Trata-se da Lei nº 13.709, de 14 de agosto de 2018, nomeada, Lei Geral de Proteção de Dados. É uma lei que se tornou necessário devido ao grande aumento do número de dados pessoais recolhidos por sites como o "Facebook", em que os usuários, para utilizar o serviço, são obrigados a fornecer informações pessoais que ficam armazenadas no banco de dados de tais empresas, e esta lei regulamenta o tratamento para com estes dados, que dizem muito sobre a pessoa física do usuário, e em alguns pontos, altera o Marco Civil da Internet (Dizer o Direito, 2018).

Ainda conforme OLIVEIRA (2014, p. 21), se o conteúdo gerado por terceiros com cenas de nudez ou de sexo causar danos, o provedor de aplicação, ao ser notificado extrajudicialmente pela vítima, tem os dois deveres: (a) o de retirar o conteúdo postado, conforme art. 20 do Marco Civil da Internet, e (b) o de informar à vítima os dados de identificação do autor do conteúdo ofensivo, como nome, CPF e endereço completo, por força do direito à informação.

Hoje, existe o consenso de nos casos de crimes cibernéticos internacionais é imprescindível a cooperação entre os países, por meio de mecanismos céleres para que se possa "*levar a bom termo*" a perseguição desta modalidade de ilícitos. Não

[7] Nome "popularmente" dado a lei, devido ao fato de grande repercussão envolvendo a atriz à época da promulgação daquela.

podendo esperar os prazos convencionais de cooperação internacional (SILVA, 2016. p. 12).

No Brasil, o comércio eletrônico tem acesso à Justiça principalmente através do Código de Defesa do Consumidor (CDC), que atualmente é previsto na Constituição Federal,

> *Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:*
>
> *[...]*
>
> *XXXII - o Estado promoverá, na forma da lei, a defesa do consumidor;*
>
> *Art. 170- A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios:*
>
> *[...]*
>
> *V-defesa do consumidor;*

Porém, conforme CANUT (2007), é necessário que se façam normas jurídicas que melhor se apliquem ao comércio eletrônico e suas diferenças do comércio de varejo tradicional em lojas físicas, desta forma, criando uma melhor proteção para o consumidor eletrônico.

Nesse sentido, em 2013 foi publicado o Decreto Lei nº 7.962, que dispões sobre a contratação em comércio eletrônico, e retrata, algumas especificidades que devem conter os sítios eletrônicos que desejam trabalhar com o comércio eletrônico.

Isto pode ser verificado principalmente no art. 4º deste Decreto, que retrata as garantias que devem o fornecedor atender,

> *Art. 4º Para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá:*
>
> *I - apresentar sumário do contrato antes da contratação, com as informações necessárias ao pleno exercício do direito de escolha do consumidor, enfatizadas as cláusulas que limitem direitos;*

> *II - fornecer ferramentas eficazes ao consumidor para identificação e correção imediata de erros ocorridos nas etapas anteriores à finalização da contratação;*
>
> *III - confirmar imediatamente o recebimento da aceitação da oferta;*
>
> *IV - disponibilizar o contrato ao consumidor em meio que permita sua conservação e reprodução, imediatamente após a contratação;*
>
> *V - manter serviço adequado e eficaz de atendimento em meio eletrônico, que possibilite ao consumidor a resolução de demandas referentes a informação, dúvida, reclamação, suspensão ou cancelamento do contrato;*
>
> *VI - confirmar imediatamente o recebimento das demandas do consumidor referidas no inciso, pelo mesmo meio empregado pelo consumidor; e*
>
> *VII - utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor. (Grifo nosso)*

Este inciso VII, foi de suma importância, pois faz com que os prestadores de serviços em comércio eletrônico desenvolvam novos mecanismos para evitar que os dados dos clientes sejam roubados de seus servidores. Porém, isso por si, não acaba com o problema das fraudes, tendo em vista, que não maioria dos casos, o roubo de dados ocorre antes mesmo de estes chegarem até o fornecedor.

De mesma maneira, o Art. 7º deste decreto insere o comércio eletrônico e a inobservância de suas regras, legalmente, dentro CDC, como observa-se "A inobservância das condutas descritas neste Decreto ensejará aplicação das sanções previstas no art. 56 da Lei nº 8.078, de 1990."

Ressalta-se também que quando houver conflito entre normas gerais e normas específicas, em regra, opta-se por aplicar a norma específica, pois existe uma noção de subsunção da norma específica dentro da geral, desta forma, a específica trataria melhor do assunto especificado. (ROVER, 2004. p. 451).

1.3 A CORRELAÇÃO DE SEGURANÇA E LIBERDADE

Para se falar em segurança e liberdade, antes devemos compreender o significado jurídico destes. Na Constituição Federal é prevista a Segurança pública em seu artigo 144, o qual discorre do dever do Estado em resguardar a segurança através dos órgãos previstos em seus incisos. Desta forma direito à segurança refere-se à necessidade de assegurar a todos o exercício dos direitos fundamentais, como o direito à vida, à liberdade pessoal, à integridade física, à inviolabilidade da intimidade, do domicílio e das comunicações pessoais, à propriedade, o direito à legalidade, à segurança das relações jurídicas.

Assim, podemos entender segurança como o dever do Estado em assegurar os direitos e garantias e desta forma manter a tranquilidade através de instrumentos que alcancem estes objetivos, sendo que por mais que o direito torne-se certo quanto a segurança, isso não necessariamente signifique uma garantia de segurança absoluta, pois é necessário que as formas de solução se renovem no decorrer dos tempos, buscando aquelas que sejam “mais adequadas à vida” (REALE, 1994).

Já Liberdade é a direito do indivíduo de poder tomar suas escolhas, decisões e praticar suas ações, dentro dos limites legais, sem ser coagido por outrem. Para que se possa ser garantida esta liberdade, o Estado cria artifícios como códigos, dispositivos e decretos, de forma a possibilitar com que o indivíduo, quando ameaçado seu direito de liberdade, possa utilizar-se destes para assegurá-lo (LEONI, 2010, p. 67).

Para Bobbio (2010) existem dois tipos de liberdade, a liberdade positiva, que consiste na liberdade coletiva, a qual é orientada pelo Estado através do dever de obediência das leis. Já a liberdade negativa seria o fazer ou deixar de fazer, dentro dos limites legais tudo aquilo que tiver vontade, é uma liberdade individual de cada um.

Com base em Constant (apud, PULIDO, 2009, p. 50) a liberdade negativa, era mais frequente nos tempos antigos, onde sua finalidade seria a de “dividir” a liberdade entres os indivíduos de uma mesma nacionalidade, enquanto a positiva é mais frequente nos tempos modernos, através da garantia do gozo privado, e dos direitos fundamentais.

Agora se faz necessário com que comparemos estes dois princípios, pois para a formação da sociedade e o fim do Estado de Natureza, foi fundamental que o ser

humano abrisse mão de suas liberdades em busca da segurança, para que assim pudessem ser formados os primeiros Estados de Direito, pois o Estado de Natureza, é um estado de guerra, e desta forma, em busca da paz, os cidadãos veem a necessidade de realizar esta troca da liberdade pela segurança (HOBBES, 2014).

Já Jean-Jacques Rousseau (2016, p. 34), fala sobre a troca da liberdade pela segurança mas não de forma direta como Hobbes, para ele o homem tem que abrir mão de suas liberdades individuais em favor da vontade geral, dando poder ao Estado Soberano, e este irá tomar as decisões em favor do bem comum, ou seja, de forma a satisfazer melhor a sociedade como um todo.

Podemos ver a relação de liberdade e segurança no comércio eletrônico através de uma perspectiva de Thomas Hobbes e de Jean-Jacques Rousseau, que analisaram correlação destes dois fatores na sociedade.

Conforme Hobbes (2014), para que os cidadãos tenham maior segurança é necessário que eles abram mão de algumas de suas liberdades individuais, ou seja, nesse caso, para sua garantia de segurança, é necessário que você abra mão da liberdade que você tem. Exemplo clássico disso são as câmeras domiciliares supervisionadas por empresas de segurança, onde para ter uma maior segurança de sua residência, você abre mão de sua liberdade (privacidade), no caso não ser filmado, em garantia da segurança, pois caso venha a ser vítima de qualquer delito dentro do recinto, as câmeras terão uma filmagem do que aconteceu.

Já Rousseau (2016), diz que a segurança e liberdade são conceitos coletivos, onde para o bem maior, ou seja, a segurança da sociedade, é necessário que os indivíduos individualmente abram mão de suas liberdades, ou seja, para que se tenha uma segurança comum[8], é necessário que todos abram mão de suas liberdades individuais.

Esses conceitos podem ser facilmente aplicados ao comércio eletrônico na atualidade, onde para garantir a segurança dos usuários, os mesmos têm de abrir mão de um pouco de sua liberdade, seja, diminuindo a comodidade, por ter de utilizar novos mecanismos de segurança e assim, consequentemente demandando um maior tempo para realizar a compra, ou aumentando o valor do produto não comprando em sites que não são confiáveis**.**

[8] Comum nesse caso foi utilizado no sentido de ser de todos ou de uma maioria, visto que alguns podem não necessitar de tal segurança.

1.3.1 Mecanismos de segurança no comércio eletrônico

Mesmo com a segurança fornecida pelas empresas, é necessário que os próprios clientes tomem algumas precauções para evitar que sejam vítimas de fraudes, para isso, existem alguns mecanismos que estes podem usar para obter uma melhor segurança de seus dados ao utilizar a internet como meio de compra (RIBEIRO et al., 2010).

Conforme Rollo (2008), o primeiro passo que os consumidores devem tomar é evitar comprar em sites desconhecidos, sempre optando por aqueles que já possuem boa reputação, e que seja bem vista por outros clientes, com críticas positivas sobre a empresa. Assim como, optar por sites nacionais, pois é mais fácil corrigir a situação caso venha a acontecer problemas na transação.

Existem algumas ferramentas, programas e aplicações que podem os usuários utilizar para sua melhor proteção, e que evitam que você sofra facilmente um golpe de fraude na internet, estes são, firewall; antivírus; antispyware; além de, ir direto ao site da empresa que deseja comprar e não acessá-lo através de links recebidos por e-mails ou qualquer outra forma; observar sempre o protocolo de comunicação[9] do site que deseja acessar; utilizar apenas seu dispositivo, seja computador ou smartphone, para realizar uma transação; não confiar em propagandas muito exageradas, pois possuem grandes chances de ser falsas (MICROSOFT, 2018), abaixo serão explicados alguns destes mecanismos.

1.3.1.1 Firewall

Firewall, conforme a Cisco (2018),

> *Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.*
>
> *Os firewalls têm sido a linha de frente da defesa na segurança de rede há mais de 25 anos. Eles colocam uma barreira entre redes internas*

[9] Protocolo de comunicação é o formato como o conteúdo do site é disponibilizado na rede.

> *protegidas e controladas que podem ser redes externas confiáveis ou não, como a Internet.*

Existem diferentes tipos de firewall, conforme sua finalidade e forma de combate às ameaças. São eles:

Firewall de Proxy foi um dos primeiros firewalls desenvolvidos, e funciona como um filtro entre uma rede e outra aplicação específica, podem oferecer alguns recursos adicionais, como, o armazenamento de dados em cache e maior segurança de conteúdo, evitando a conexão com outros computadores fora da rede, porém, isto pode apresentar problemas na comunicação com outros programas que queira utilizar (CISCO, 2018).

Firewall com inspeção de dados, são os firewalls comuns dos computadores, ele funciona a partir da inspeção, bloqueando ou permitindo o tráfego de dados, dependendo do estado, porta e protocolo das conexões. Monitora toda a conexão, e o filtro do firewall é realizado conforme o definido pelo administrador e contexto da conexão, que neste caso significa anterioridade de obtenção de dados de uma mesma conexão (CISCO, 2018).

Firewall de Gerenciamento Unificado de Ameaças (UTM), funciona normalmente, combinando a inspeção de dados, prevenção contra intrusos e antivírus. É um firewall que protege também os dados em nuvem[10], e tem foco na simplicidade e facilidade para os usuários.

Por fim, o Firewall de Próxima Geração (NGFW), que conforme a Cisco (2018),

> *Os firewalls evoluíram para além da simples filtragem de pacotes e inspeção stateful. A maioria das empresas está implantando firewall de próxima geração para bloquear ameaças modernas, como malware avançado e ataques na camada da aplicação.*
>
> *De acordo com a definição do Gartner, Inc., um firewall de próxima geração deve incluir:*
>
> - *Recursos padrão de firewall, como inspeção stateful*
> - *Prevenção de invasão integrada*
> - *Reconhecimento e controle da aplicação para detectar e bloquear aplicativos nocivos*

[10] Armazenamento em nuvem é o armazenamento de dados na rede utilizando a rede de computadores e servidores interligados por meio da internet, ou rede particular.

> - *Atualização de caminhos para incluir feeds futuros de informação*
> - *Técnicas para lidar com as ameaças à segurança em evolução*
>
> *Embora esses recursos estejam se tornando cada vez mais a norma para a maioria das empresas, os NGFWs podem fazer mais.*
>
> *NGFW focado em ameaças*
>
> *Esses firewalls incluem todos os recursos de um NGFW tradicional e também oferecem detecção e remediação avançadas de ameaças. Com um NGFW focado em ameaças, você pode:*
>
> - *Saber quais recursos sofrem um risco maior com reconhecimento completo de contexto*
> - *Reagir rapidamente a ataques com automação de segurança inteligente que define políticas e fortalece suas defesas de forma dinâmica*
> - *Detectar melhor as atividades evasivas e suspeitas com a correlação de eventos de rede e endpoint*
> - *Reduzir expressivamente o tempo entre a detecção e a limpeza com segurança retrospectiva que monitora continuamente atividades e comportamentos suspeitos mesmo após a inspeção inicial*
> - *Facilitar a administração e reduzir a complexidade com políticas unificadas que oferecem proteção durante todo o ciclo de ataque*

1.3.1.2 Antivírus

Antivírus é um software de computador, com aplicação também em outros dispositivos eletrônicos, que tem a finalidade de detectar, evitar, neutralizar e remover alguns tipos de malwares do dispositivo, como vírus, worms e trojans. Para que seu antivírus continue a proteger seu dispositivo contra os novos malwares que vão surgindo é necessário sempre mantê-lo atualizado (MICROSOFT, 2018).

Existem também os antivírus de nuvem, que conforme a Kaspersky (2018), podem ser definidos como,

> *Antivírus na nuvem é uma solução que transfere cargas de trabalho antivírus para um servidor na nuvem, em vez de sobrecarregar o computador do usuário com um pacote antivírus completo. Enquanto os programas de segurança tradicionais dependem do poder de processamento do computador local de um usuário, as soluções de computação na nuvem instalam apenas um pequeno programa "cliente" no computador que, por sua vez, conecta-se ao serviço Web do provedor de segurança. Ali, os dados das verificações antivírus são*

> *analisados, e as instruções para que sejam tomadas as medidas apropriadas são enviadas de volta ao computador do usuário.*

1.3.1.3 Antispyware

Conforme a Microsoft (2018), o software antispyware protege o seu computador contra os spywares, que geralmente são projetados para ser de difícil remoção, não bastando apenas que você exclua esse malware do sistema, mas sim faça uma limpeza com um antispyware, pois com sua simples exclusão, os spywares costumam retornar ao sistema assim que o mesmo é reiniciado.

No mesmo sentido, a empresa Kaspersky (2018), também diz,

> *Uma solução antispyware eficiente é capaz de remover o spyware facilmente e garantir que ele seja completamente eliminado. Depois de executar o software antispyware, observe a operação do sistema. Verifique os processos, saiba o que está sendo executado e verifique se as configurações do firewall estão corretas.*

1.3.1.4 Proxy

Outro mecanismo que pode ser utilizado é o proxy, que restringi os dados e seu tráfego na rede de computadores. Ele funciona através do controle de dados na rede, restringindo e permitindo a comunicação de dados entre diferentes computadores. É um método utilizado principalmente em empresas com a finalidade de ter um controle do uso de seus computadores pelos funcionários, garantindo assim, uma maior segurança, e também produtividade, pois podem bloquear aqueles destinos que venham a tirar o foco deles (HAUTSCH, 2010).

Através TCP/IP nas redes locais, assume o proxy a função de retransmitir os dados através de “pontes estreitas” e *routers*. Com o uso de proxys é possível acompanhar os registros de rede e assim, analisar os pedidos dos clientes e respostas dos servidores (CCM, 2018).

1.3.1.5 Certificado digital

É um documento eletrônico constituído por um nome e número individual, o qual dá-se o nome de chave pública. É aplicado para garantir uma maior segurança

aos sites em envios de mensagens e em transações comerciais por meios eletrônicos, por este motivo, empresas vêm solicitando cada vez mais seu uso (RESENDE, 2009).

No comércio eletrônico, o certificado digital mais utilizado é o SSL, que confirme a Active Web (2018), empresa de segurança digital,

> *O SSL (Secure Sockets Layer) é um protocolo de segurança que se tornou padrão internacional para troca de informações sigilosas na Internet.*
>
> *Um Certificado Digital é um arquivo de computador que contém um conjunto de informações referentes à entidade para a qual o certificado foi emitido (seja uma empresa, pessoa física ou computador) mais a chave pública referente à chave privada que se acredita ser de posse unicamente da entidade especificada no certificado.*
>
> *O Certificado SSL possibilita a criação de um canal seguro entre um servidor web (site, sistema, webmail, etc) e o seu navegador, garantindo que todos os dados trafegados estejam protegidos e não possam ser interceptados.*
>
> *Com a utilização do Certificado SSL é possível mostrar visualmente que o seu site é confiável, autêntico e não clonado. Além da segurança, o Certificado SSL aumenta o ranking do seu site nas buscas do Google.*
>
> *O Certificado SSL é essencial para todos os tipos de sites, principalmente para empresas de comércio eletrônico, que precisam proteger dados como informações de cadastro e números de cartão de crédito dos clientes*

1.3.1.6 Criptografia

É a conversão de dados para um formato codificado que só pode ser utilizado após ser descriptografado. Atualmente é um elemento de extrema importância na segurança de dados quando falamos em computação e internet, isso porque, além de serem em alguns casos, de simples uso, evita que esses dados sejam facilmente acessados por qualquer pessoa.

Amplamente utilizada, a criptografia atende à necessidade desde grandes empresas, que necessitam de alta criptografia, até o usuário individual que utilizam em geral uma criptografia mais simples. Neste mesmo sentido, a criptografia também atende diferentes áreas na internet, desde proteção de dados sigilosos de uma empresa, até o pagamento no comércio eletrônico (KASPERSKY, 2018).

Conforme Eric Moreira (2018),

> *Uma criptografia bem elaborada dificulta até mesmo a realização de investigação policial. Foi através deste tema que se criou a "criptografia responsável", tão bem conhecida como backdoor, maneira a qual governos e, obviamente, hackers, tem acesso aos dados criptografados.*

Atualmente, a forma de criptografia que vem sendo bastante utilizada é a AES 256, que atua em conexões via IP e servidores, está ferramenta de criptografia evita que intrusos, que não tenham a autorização de acessar os dados protegidos consigam utilizar os dados armazenados. Com ferramentas como essa, torna-se cada vez mais segura a transmissão de dados via internet, e com isso, novas janelas de possibilidades vão surgindo dentro do meio eletrônico (MOREIRA, 2018).

Eric Moreira (2018), ainda complementa sobre o momento atual da proteção de dados na internet,

> *Nota-se que as tecnologias de criptografia de dados avançadas de sistemas e dispositivos de rede se tornam essenciais para reduzirem os riscos associados com perda ou roubo de dados, garantindo o gerenciamento centralizado seguro de dispositivos variados local ou remoto. O presente momento pede que as empresas considerem os custos relacionados à proteção de rede para garantir a confiabilidade e credibilidade de sua marca dentro de um mercado cada vez mais competitivo ao mesmo tempo que dispõe ao usuário o compromisso de manter seu ambiente efetivamente seguro.*

1.3.2 Liberdade no comércio eletrônico

As liberdades no comércio eletrônico podem ser vistas também como suas vantagens, que são traduzidas em mais opções para o consumidor, negociar com qualquer lugar do mundo sem precisar sair de casa, comprar a qualquer hora do dia, mais opções e facilidades de pagamento, além de, uma maior liberdade financeira para o fornecedor, que com menos custos, pode disponibilizar um produto com menor valor, e assim, tornando-o mais acessível ao consumidor (ARROYO, et al, 2006).

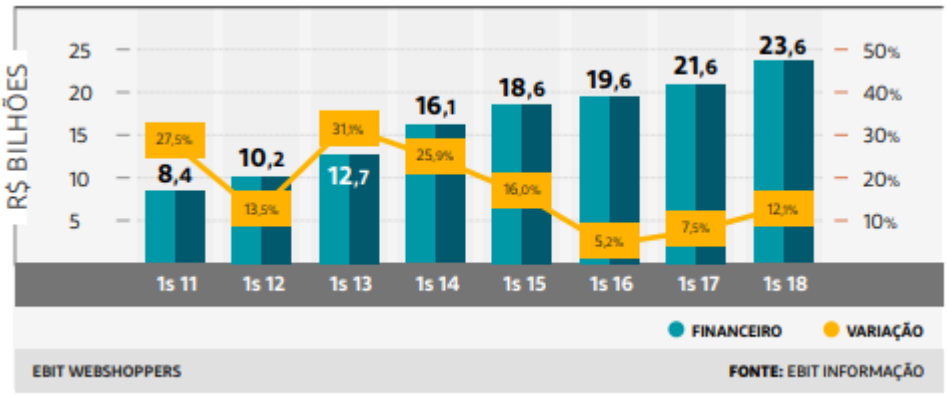
Corroborando isso, Reedy e Schullo (2007), falam que o comércio eletrônico pode proporcionar novas liberdades tanto ao consumidor, quando ao fornecedor, como, um menor custo para a abertura de uma loja virtual, em relação a uma loja física; uma maior flexibilidade quanto a operação da loja, facilitando assim, o funcionamento desta, 24 horas por dia; uma melhora na imagem da empresa, assim como maior divulgação virtual dela; testes de novos produtos, serviços e tecnologias.

2 APRESENTAÇÃO E FUNDAMENTAÇÃO DA PROPOSTA

2.1 ESTUDO DE CASO: O CRESCENTE NÚMERO DE USUÁRIOS REALIZANDO COMPRAS POR INTERMÉDIO DA INTERNET

Conforme dados do eBit[11], obtidos através do Webshoppers 38[12] no primeiro semestre de 2018, 27,4 milhões de usuários realizaram compras pela internet, e destes, 4,5 milhões realizaram sua primeira compra online. Além disso, é previsto para o ano de 2018, um faturamento de R$53,4 bilhões somente no comércio eletrônico, o que representa um aumento de 12% em relação ao ano de 2017, conforme gráfico 1.

Gráfico 1 - Faturamento das vendas online nos primeiros semestres anuais



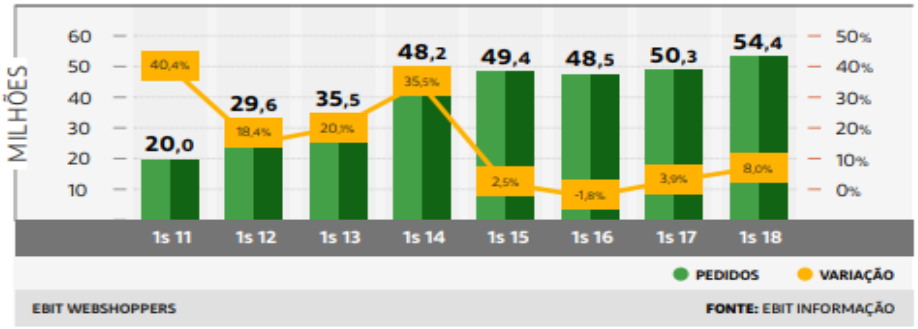
Fonte: Ebit, 2018.

O número de pedidos também cresceu, conforme pode ser visto no gráfico 2 abaixo, passando de 50,3 milhões no primeiro semestre de 2017 para 54,4 milhões de pedidos no primeiro semestre de 2018, ocasionando num aumento de 8,2%.

[11] eBit é uma empresa brasileira que analisa os dados de e-commerce no Brasil. ela é pertencente a Nielsen Holdings plc, que é responsável pela mensuração e análise de dados, com a maior confiabilidade e complexidade no mundo.

[12] Webshoppers é atualmente o relatório de maior credibilidade de dados do comércio eletrônico no Brasil, sendo realizado desde 2001.

Gráfico 2 - Número de pedidos no comércio eletrônico nos primeiros semestres anuais.



Fonte: Ebit, 2018.

Como podemos notar nos gráficos acima, esta evolução não é apenas no último ano, mas algo que vem crescendo gradualmente ao longo dos anos, e que possui perspectivas para continuar aumentando.

Segundo pesquisa realizada pela Google, divulgada em outubro de 2016, a previsão é que para o ano de 2021 o número de usuários a realizar compras online seja de 67,4 milhões, cerca de 44% do número de usuários conectados à internet no Brasil, e a faturação anual através deste meio alcançará os R$85 bilhões.

O segmento de compras online tem se tornado tão presente no Brasil, que conforme pesquisa da PWC[13] (2016), divulgada no “Total Retail 2016”, apontou-se que 38,2% dos brasileiros realizam compras todos os meses através do comércio eletrônico, enquanto 30,9% efetuam compras em lojas físicas mensalmente. Desta forma, o comércio eletrônico começa a se tornar não mais a segunda opção de compras, mas sim, a tomar o posto principal de vendas em nosso país.

Ainda conforme o Total Retail 2016, o segmento onde se tem uma maior “dominância” do comércio eletrônico sobre as lojas físicas é o de vendas de eletrônicos, e o de livros, músicas, filmes e videogames, onde 60% e 71% dos consumidores, respectivamente, preferem realizar a compra on-line. Porém, em segmentos como o de alimentos e materiais de construção, ainda se mantém uma dominância das lojas físicas.

Porém, essa evolução não é de hoje, após seu surgimento em 1995, e ter passado por um momento onde não se via um efetivo potencial na internet como vemos hoje em dia, permanecendo assim até 2000, quando começou-se a ter um maior investimento nas vendas online, porém, com restrições, visto que os

[13] PWC, ou PricewaterhouseCoopers, é uma empresa prestadora de serviços profissionais de auditoria, consultoria e outros serviços acessórios para empresas.

investidores tinham receio em investir nesse novo comércio ainda incerto, e que demonstrava um risco de não dar o retorno esperado em relação a seu investimento (ALMEIDA; BRENDLE; SPINOLA, 2014).

Seu crescimento efetivo se deu a partir do ano de 2002, quando o comércio eletrônico faturou R$850 milhões em território nacional, o que começou a dar um novo rumo ao mercado virtual, que se confirmou no ano de 2003, quando com um aumento de 41% em relação ao ano anterior, o comércio eletrônico faturou R$1,2 Bilhões. Acabou se concretizando no ano de 2008, quando em meio a uma crise financeira, conseguiu fechar o ano em alta e com um faturamento de R$8,2 Bilhões, e ainda, alcançar um aumento de 30% no ano seguinte, alcançando a marca de R$10,6 Bilhões (GUASTI, 2010).

A partir de 2011, como podemos verificar no gráfico 2, com dados do Ebit, o crescimento começou a diminuir relação a proporção que vinha crescendo, mas se manteve, apresentando do primeiro semestre de 2011 ao primeiro semestre de 2017 um aumento de 172% no número de pedidos, além de 180,95% de crescimento em faturamento, resultando em R$15,2 bilhões.

Desta forma podemos verificar que o cenário atual do comércio eletrônico, em relação ao faturamento de 2002 que era de R$850 milhões aumentou 6.182,35%, se levarmos em considerarmos o valor estimado de R$53,4 bilhões de faturamento para 2018 e compararmos o crescimento de 2002 a 2018.

Ressalta-se, que nestes valores não são incluídos aqueles arrecadados por negociações realizadas através dos *marketplaces*, como por exemplo, o Mercado Livre, que no ano de 2017, apresentaram um faturamento de R$73,4 bilhões, na venda de novos e usados, o que representou um aumento de 21,9% em relação a 2016 (EBIT, 2017).

Conforme estudo realizado por Miranda e Arruda (2004), através de uma pesquisa direta com 198 consumidores que utilizam o comércio eletrônico, constatou-se que são vários os motivos que levam o consumidor a realizar a compra online ao invés de em lojas físicas. Como podemos ver nos resultados apresentados pelas pesquisadoras:

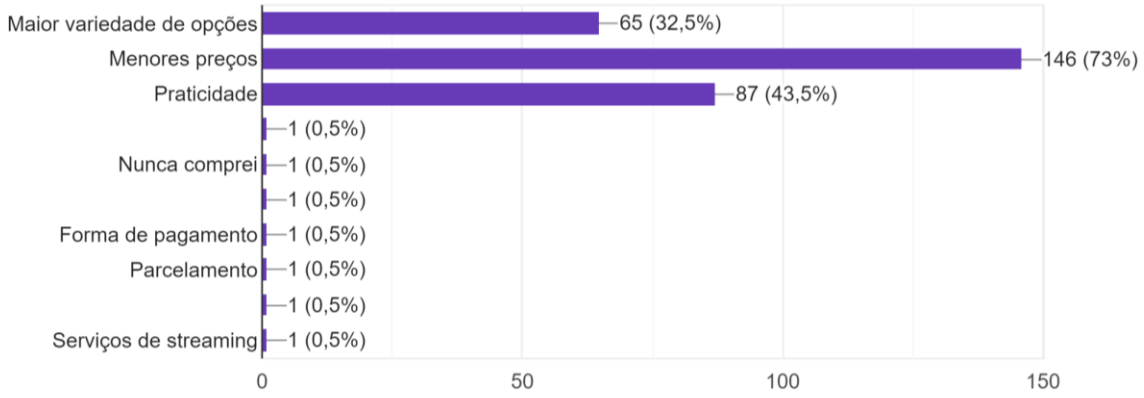
> *É importante mencionar que, no mínimo, 67% dos respondentes, consideram os atributos Facilidade e Rapidez de Navegação, Acesso a Produtos não Encontrados no Mercado, Presença de Ferramentas de Segurança, Qualidade e Variedade dos Produtos Ofertados,*

> *Entrega no Prazo Previsto, Presença de um Canal de Serviço e Preço Inferior às Outras Formas de Comércio de alta importância para a decisão de compra no varejo virtual, cujas medianas encontradas variam entre 4 e 3. Desta forma, não devem ser desprezados pelos profissionais de marketing.*

Porém, o principal motivo é a comodidade que este tipo de compra oferece, ou seja, o fato de você poder realizar a compra a qualquer hora do dia e de não precisar se deslocar para realizá-la, bastando ter um dispositivo e acesso à internet.

Colaborando com isso, em pesquisa de autoria própria e elaborada para complemento desta monografia, através da aplicação de questionário, contando com um grupo de 200 participantes, cujo resultado está disposto no gráfico 3, o principal motivo que leva os consumidores a utilizar o comércio eletrônico é o menor preço do produto em relação à loja física (73%), seguido de praticidade (43,5%) e maior variedade de opções (32,2%).

Gráfico 3 - Motivos para utilizar o comércio eletrônico.



Fonte: Pesquisa elaborada pelo autor.

Em contraponto, os principais motivos que levam as pessoas a não comprar na internet são a preferência pela loja real, o fato de o consumidor não gostar de realizar a comprar sem antes ver e poder tocar ou sentir o produto a ser comprado, a não confiança nas ferramentas de segurança utilizadas (MIRANDA; ARRUDA, 2004).

2.2 O AUMENTO DOS CONFLITOS NO COMÉRCIO ELETRÔNICO

Conforme estudos feitos pela Clear Sale[14], e divulgados em seu “Mapa da Fraude”, que tem por objetivo verificar as tentativas de fraudes realizadas em comércio eletrônico no território brasileiro, no ano de 2017, 3,42% do valor total arrecadado foi fruto de fraudes em compras, ou seja, dos R$47,7 bilhões que foram faturados em 2017, conforme o 37º Webshoppers, da empresa Ebit, aproximadamente R$1,63 bilhões foram objeto de fraude.

Este valor representa um aumento de 14% no número de fraudes quando comparado com o ano de 2016 (Clear Sale, 2018), sendo que, no mesmo período, o comércio eletrônico cresceu apenas 7,5% (Ebit, 2017).

Para Leandro de Carvalho Alves, Fabiolla Valeria Gonçalves e Luzelia Calegari Santos Moizinho (2013),

> [...] é basilar que a contabilização dos custos com fraudes seja monitorada pelas organizações com eCommerce e que estes sejam tratados como qualquer outro custo do negócio. A mensuração das perdas pode ser altamente rentável na medida em que os esforços para reduzir os prejuízos são proporcionais ao conhecimento no tocante ao problema. Embora exista o custo com a infraestrutura para minimizar as fraudes, o autor argumenta que os benefícios gerados por informações precisas sobre a natureza e extensão da fraude são compensatórios e conclui que a fraude deve ser tratada com uma abordagem holística e em alguns setores como uma vantagem competitiva.

Este aumento do comércio eletrônico, conforme o Superior Tribunal de Justiça[15] (2018), acaba por criar uma nova demanda dentro do Judiciário, sendo necessário o constante posicionamento dos ministros em relação aos tipos de fraudes que vem acontecendo, a exemplo, a não entrega do produto. Este fato pode ser averiguado a partir do que diz o próprio tribunal em notícia divulgada em sua página:

---

[14] Clear Sale é uma empresa especializada em serviços antifraudes para comércio eletrônico.

[15] Superior Tribunal de Justiça, ou STJ, é o órgão do Poder Judiciário brasileiro que tem a finalidade de garantir a uniformidade quanto à interpretação das legislações federais.

> *O crescimento é constante, registrando taxas superiores a 10% no comparativo com o ano anterior. O novo hábito do consumidor brasileiro gera mudanças na legislação e discussões no Poder Judiciário.*

De mesma forma, SILVA (2015), em seu artigo sobre o acesso ao judiciário no comércio eletrônico, afirma que,

> *Atualmente o comércio eletrônico é um dos principais focos de litígios judiciais, seja pela insuficiência da lei em determinadas práticas no mundo virtual ou pela própria vulnerabilidade do consumidor.*
>
> *Não há dúvida que o aumento da porcentagem de litígios no judiciário, em relação consumerista, é provocado pelas fraudes, abusos falha na prestação de serviço no comércio eletrônico*.

2.3 O PERFIL DO ATUAL USUÁRIO DO COMÉRCIO ELETRÔNICO

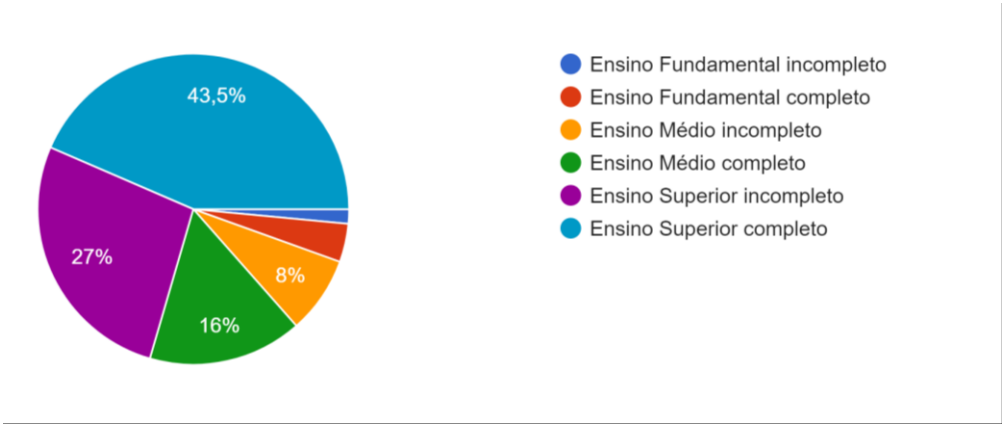
Conforme o Ebit (2018), o e-consumidor brasileiro possui uma média de idade de 43 anos, sendo que, 68,2% das compras são realizadas por usuários com mais de 35 anos. Este fato é contrário ao perfil do e-consumidor de outras regiões do mundo, como a Europa, onde a maior parte das compras é realizada por usuários entre 19 e 29 anos, o que pode ser justificado pelo fato dos jovens brasileiros geralmente não possuir uma estabilidade financeira (LOPEZ, 2018).

Quanto a classe social[16], o consumo eletrônico é realizado principalmente pela classe média e média baixa (C e D respectivamente, conforme classificação do IBGE), as quais representam 65,8% do consumo em comércio eletrônico no Brasil, por outro lado, as classes alta e média alta (A e B respectivamente), consomem apenas 17,8% deste mercado, ficando os outros 16,4% representados pela classe baixa (E) (EBIT, 2018).

Quanto à escolaridade, através de pesquisa própria, obteve-se que 70,5% dos participantes da pesquisa possui Ensino Superior Completo ou Incompleto, gráfico 4, fato este que pode ser resultado do meio social, acadêmico, em que a pesquisa foi realizada.

[16] Conforme o IBGE, as classes sociais brasileiras são divididas em A, renda mensal acima de 15 salários mínimos; B, entre 5 e 15 salários mínimos; C, entre 3 e 5 salários mínimo; D, entre 1 e 3 salários mínimos; e E, abaixo de 1 salário mínimo.

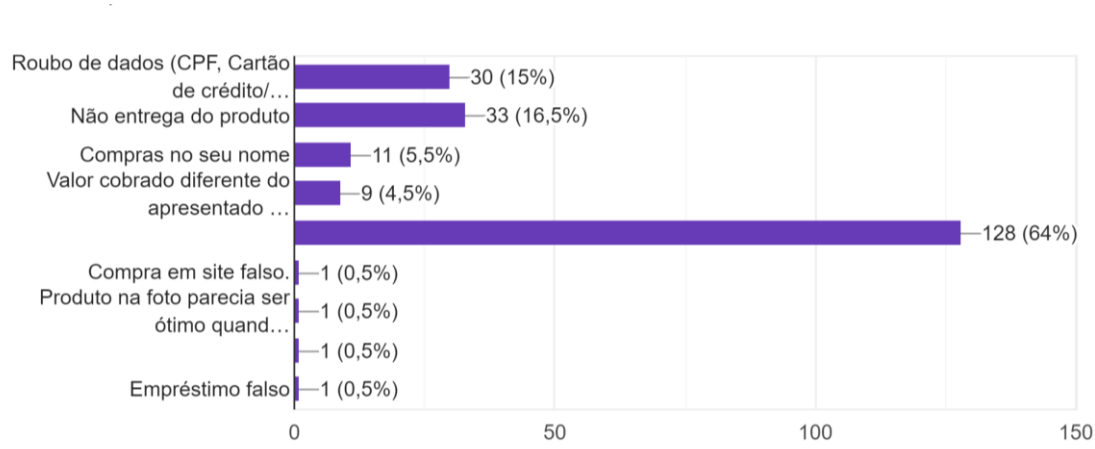
Gráfico 4 - Escolaridade



Fonte: Pesquisa elaborada pelo autor.

Por outro lado, o número de participantes que foram vítimas de fraude é de 72 (36%), sendo que destes, 30 (15%) foram vítimas de roubo de dados, e 33 (16,5%) da não entrega do produto, conforme observamos no gráfico 5, enquanto 128 (64%) participantes alegaram nunca ter sido vítima de fraude. Esse número é bastante elevado, pois representa mais de um terço dos participantes, e demonstra que o fator escolaridade não é tão significativo quando submetido a ser ou não vítima de fraudes.

Gráfico 5 - Vítimas de fraude.

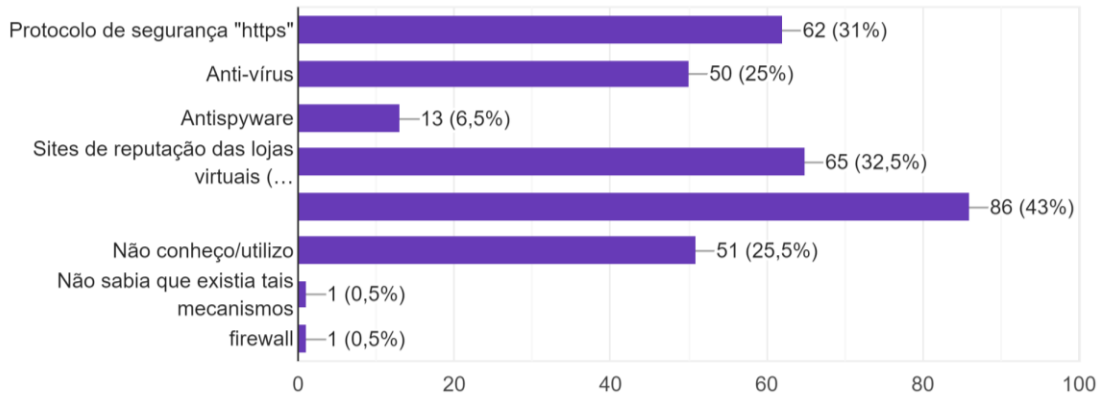


Fonte: Pesquisa elaborada pelo autor.

Conforme levantamento de 2015, 28% dos consumidores online havia sido vítimas de fraudes, o que demonstra que os resultados obtidos na pesquisa não estão longe da realidade do comércio eletrônico no Brasil. O que é muito preocupante, pois isso faz com que estes que foram vítimas tenham uma tendência a mudar seus hábitos, e começar a evitar utilizar o comércio eletrônico novamente, com medo de tornar a ser novamente vítima de fraudes (OBERTHUR TECHNOLOGIES apud E-COMMERCE BRASIL, 2016).

Outro fator relevante, é que conforme dados obtidos na pesquisa, e dispostos no gráfico 6, 51 participantes (25,5%) relatou não utilizar nenhum mecanismo de segurança ao realizar compras na internet, assim como, 50 (25%) e 13 (6,5%) relatam utilizar antivírus e antispyware, uma parcela muito pequena que pode refletir o grande número de fraudes. Por outro lado, os mecanismos mais utilizados são reputação da loja (32,5%), protocolo de segurança do site (31%) e comentários de outros consumidores (43%), que apesar de serem efetivos quanto a segurança do local em que se está comprando, se não conciliados com outros mecanismos que façam a proteção do seu dispositivo acabam não evitando que você torne-se vítima de fraudes.

Gráfico 6 - Uso de mecanismos de segurança por parte dos consumidores.



Fonte: Pesquisa elaborada pelo autor.

2.4 A NECESSIDADE DE NOVOS MECANISMOS DE SEGURANÇA

O número de fraudes vem aumentando anualmente e alguns fatores contribuem diretamente para que estes ocorram, como o aumento da quantidade de

dados de cartões de crédito circulando virtualmente, uma constante evolução tecnológica, a qual pode representar pontos positivos e também negativos no comércio eletrônico e na sociedade, e principalmente a falta de cuidado do usuário ao realizar compras pela internet (GLOBAL CONSUMER CARD FRAUD, 2017).

O fato de o consumidor não ter o conhecimento, ou não fazer o uso dos mecanismos de segurança disponíveis, conforme exposto no gráfico 6, demonstra que, mesmo com mecanismos que são eficazes, quando seu uso não é obrigatório, e depende somente do usuário, muitos por não conhecimento ou até por descuido, acabam não se utilizando destes mecanismos e vindo a se tornar vítimas. Com isso, surge a necessidade de novos mecanismos que sejam de uso obrigatório, e requisitados pelas próprias lojas virtuais.

Nesse sentido afirmam Albertin e Moura (1998),

> *Enquanto assinaturas digitais, firewalls, algoritmos de criptografia e senhas podem auxiliar a proteger nossos direitos, eles não são suficientes. Procedimentos e práticas atuais de segurança, privacidade e integridade de informação precisam ser examinados e as políticas de informação e comunicação interorganizacionais precisam ser estabelecidas. Regulamentações governamentais e aspectos legais precisam ser tratados.*

Segundo Fagundes (2014), quanto mais avançamos na tecnologia, mais riscos vão surgindo, e com isso, torna-se necessário que surjam novas medidas de segurança para se proteger desses riscos. Não podemos investir apenas na proteção das áreas de TI, devem ser feitos investimentos em novos mecanismos de segurança também na área do comércio eletrônico, prevenindo-a contra fraudes e falhas de segurança. Deve-se tomar o uso das novas tecnologias, como Big Data[17], também em razão da proteção de dados nesta área.

Conforme Canabarro (2014), além de diminuir a incidência de fraudes, e desta forma, trazer mais segurança para o comércio eletrônico, um sistema antifraude eficaz impulsiona o mercado também de outra forma. Nos atuais sistemas, compradores novos, ou de localidades onde a proporção de fraudes acometidas é maior, possuem uma maior dificuldade em terem suas compras aprovadas, ou seja, em meio ao combate à fraude, muito compradores potenciais são barrados de realizar suas

[17] Tecnologia para armazenamento de grandes volumes de dados com grande velocidade de acesso.

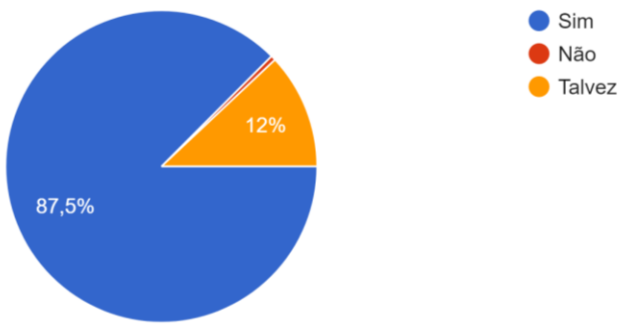
compras, desta forma, com um sistema eficaz, eles poderiam realizar as compras autenticando-as, e desta forma, o mercado seria impulsionado, pois novos compradores potenciais, que no atual sistema são impedidos de realizar compras, conseguirão fazê-las.

Assim como os avanços tecnológicos são favoráveis aos consumidores, eles também oferecem novas possibilidades aos fraudadores que também se beneficiam destes avanços, em relação a isto, Breeden (2017) afirma,

> *Os fraudadores sempre terão os canais mais fracos como meta, portanto é preciso controlar os riscos em todos os ambientes. É imprescindível criar e manter mais níveis de validação de identidade (autenticação) para realizar transações, além de senhas mais fortes e seguras e uso de inteligência artificial, pois fraudadores também sabem que a maioria das pessoas utiliza senhas mais simples, até mesmo para lembrar com facilidade.*

Esse é um sentimento compartilhado também por a maior parte dos usuários que fizeram parte de pesquisa elaborada, onde ao perguntar se estes viam necessidade em se criar novos mecanismos de segurança para o comércio eletrônico, os resultados, gráfico 7, demonstraram que a grande maioria, 175 (87,5%) dos participantes totais, vê necessário esse investimento.

Gráfico 7 - Necessidade de novos mecanismos de segurança.



Fonte: Pesquisa elaborada pelo autor.

Albertin e Moura (1998) ainda afirma que,

> *[...] para comércio eletrônico é importante que os clientes se autentiquem para os servidores, que os servidores se autentiquem para os clientes e que ambos se autentiquem um ao outro. A autenticação é um mecanismo pelo qual o recebedor de uma transação ou mensagem pode ter certeza da identidade do emissor e/ou da integridade da mensagem. Em outras palavras, a autenticação verifica a identidade de uma entidade, um usuário ou um serviço, utilizando certas informações criptografadas transferidas do emissor para o destinatário.*

As ameaças do crime eletrônico acabam por comprometer os avanços no comércio eletrônico, apresentando de forma a limitar o potencial que esse mercado possibilita para a economia. Vão além de problemas tecnológicos, pois em virtude dessas ações delituosas no âmbito virtual, temos consequências na economia, devendo assim, tratar estas fraudes também como um problema financeiro (SMITH, et al., 2011).

2.5 PROPOSTA PARA A DIMINUIÇÃO NA INCIDÊNCIA DE FRAUDES NO COMÉRCIO ELETRÔNICO

Visto o exposto acima, faz-se necessário que novos mecanismos de segurança sejam necessários para garantir a segurança dos consumidores na hora de realizar a compra virtual, assim como uma “educação” dos consumidores quando a realização de compras online, porém, este último é algo que podemos considerar não aplicável, vistas as diferentes características dos consumidores, principalmente em relação à faixa etária e escolaridade.

Desta forma, propõe-se uma alteração no Decreto-Lei 7.962/2013, para incluir em seu texto o desenvolvimento e disponibilização de novos mecanismos de segurança, que atuem na proteção dos dados do consumidor também durante o ato de realização da compra. Pois apesar de hoje existirem mecanismos com tais finalidades, muitas pessoas não possuem o conhecimento destes.

Neste sentido propomos dois mecanismos em específico que poderiam trazer uma melhora na compra. O primeiro é o uso de código de confirmação de compra, que o consumidor receberá através de um SMS, e só após sua inserção no campo destinado a compra poderá ser confirmada. O segundo seria a utilização de softwares

que impeça a comunicação do dispositivo do consumidor com outros, que não sejam o da loja virtual, no momento da compra.

2.5.1 Confirmação de compra via SMS

Este mecanismo já é utilizado em alguns sites de compra no exterior, assim como por alguns bancos e cartões de crédito aqui no Brasil, porém, com aplicabilidade em um número reservado de sites de compras.

O serviço, é basicamente a confirmação da compra através de um SMS que será enviado pela sua agência bancária. Neste caso, o consumidor, após informar seus dados, como CPF e Número do Cartão de Crédito, no site de compras é direcionado para uma tela onde deverá inserir um código que será enviado a seu número de celular, que está cadastrado junto a sua agência bancária, e apenas após a informação correta deste código a compra poderá ser finalizada. Este mecanismo ajuda a evitar que outras pessoas, na posse de seus dados, realizem compras com estes, pois, será necessária uma confirmação mecânica do usuário através da inserção do código, que na maioria destes casos de fraude, não terá acesso ao celular do indivíduo que teve seus dados roubados, evitando assim, que a compra se concretize.

O Banco Santander oferece um serviço similar a este proposto, que é o Token Santander, onde sempre que qualquer transação envolvendo sua conta é realizada o banco envia para o *token*[18] do cliente um código para que ele confirme a transação. Conforme o próprio Santander (2018),

> *Token é um dispositivo eletrônico de segurança que garante ainda mais proteção às transações financeiras efetuadas pelo Internet Banking Empresarial. Ele impede que programas maliciosos possam capturar as informações digitadas, garantindo que seu acesso seja seguro e confidencial.*

Outro serviço similar a este é o *3-D Secure*, que no Brasil é disponibilizado pela MasterCard e pela Visa, com o *Mastercard Secure Code* e o *Verified by Visa* respectivamente. Porém, estes serviços dependem de um pedido expresso do cliente,

[18] Token é um dispositivo eletrônico gerador de senhas.

que vai assinar o serviço, e além disso, não é compatível com todos as lojas online. O funcionamento destes serviços é através de alguns passos, conforme a Visa (2018),

> 1. *Vá à loja online que deseja comprar um produto.*
> 2. *Siga o processo de compra do site.*
> 3. *Selecione pagar com seu cartão de débito Visa Electron ou seu cartão de crédito Visa.*
> 4. *Preencha os dados solicitados.*
> 5. *Ao seguir para a próxima tela, você será direcionado para o ambiente seguro do seu banco.*
> 6. ***Confira as informações referentes à sua compra e forneça os dados solicitados pelo banco, que podem ser: tabelas com códigos de segurança, token eletrônico, mensagens via SMS ou dados que somente você e seu banco conhecem.***
> 7. *Após o seu banco validar os dados digitados, sua compra será validada.*
> 8. *Em breve a loja confirmará seu pedido. (Grifo nosso)*

São protocolos de segurança interbancários que garantem alta segurança para pagamentos on-line, funcionam através da autenticação da identidade do portador do cartão de crédito que está sendo utilizado para realizar a compra. É o mecanismo com o mais alto nível de segurança disponível hoje (PAYZEN, 2018).

PayZen (2018) detalha também o uso deste mecanismo,

> *A autenticação ocorre após a digitação dos dados de cartão de crédito ou débito. Nesta hora, o cliente visualiza na página de pagamento uma pergunta de seu banco (geralmente a digitação de um código de* token*, seja de tipo chaveiro, seja de tipo aplicativo smartphone ou ainda recebido por SMS). A resposta positiva a essa pergunta no ambiente seguro do banco permite validar definitivamente a identificação do comprador e, imediatamente depois, do pagamento.*

Conforme Martínez López,

> *Adoptar 3-D Secure es fácil y sencillo para comerciantes y compradores. Los vendedores no tienen que modificar sus aplicaciones de venta, sólo instalar un plug-in en sus servidores de comercio electrónico y adquirir un certificado que les identifica como tienda confiable. Por su parte, los usuarios compradores no tienen la necesidad de instalar ningún software ni adquirir dispositivo alguno*

> *para disfrutar de las ventajas de 3-D Secure. Sólo deben tramitar su contraseña con el banco emisor de su tarjeta de crédito Visa que utilizan normalmente en cualquier mercado tradicional. Sin embargo, este protocolo no es totalmente infalible, ya que han aparecido algunas críticas respecto a su implantación. Una de ellas es la dificultad que encuentran los usuarios para distinguir entre una ventana emergente legítima de Verified by Visa y una fraudulenta de phising.*

Ou seja, o uso do 3-D Secure, é um sistema que tem muito a acrescer ao sistema de segurança do comércio eletrônico, sem apresentar grandes dificuldades de aplicação nas atuais lojas virtuais, sendo necessário somente a instalação de um plug-in nos servidores destas lojas. Além disso, por mais que não se trate de um sistema totalmente imune a fraudes, ele facilmente lida com um dos principais métodos utilizados pelos fraudadores, que é o *phishing*, pois mesmo com os dados da vítima, não haverá como o fraudador realizar a autenticação mecânica que este mecanismo de segurança exige.

Desta forma, o proposto seria tornar este, um serviço obrigatório, sendo necessária a adaptação de todas as lojas virtuais para este serviço, assim, como uma adequação dos bancos para passar a fornecer somente os cartões de crédito que disponibilizam tal serviço, sendo necessário que as bandeiras que não o forneça passem a fornecer.

2.5.2 Uso de programas que evitem a conexão do usuário com outros dispositivos enquanto realiza a compra

Este serviço funcionaria de forma a evitar que o roubo de dados ocorre-se através de malwares que transmitem os dados do usuário enquanto estão sendo digitados para outros dispositivos eletrônicos.

Atualmente, existem alguns softwares que fazem tal serviço e que são utilizados por alguns bancos, a exemplo, o *Warsaw,* desenvolvido pela GAS Tecnologia, que é utilizado pelo Banco do Brasil, pela Caixa Econômica Federal e outros bancos.

O *Warsaw* funciona através do bloqueio de outros endereços de IP que tentem se comunicar com o seu dispositivo enquanto o programa está em uso, desta forma evitando que outras pessoas tenham acesso ao seu dispositivo naquele momento.

Conforme a Agility Networks (2016),

> *Existem soluções como o módulo de segurança Warsaw da GAS, aplicativo cliente que deve ser instalado na máquina do usuário antes do acesso à aplicação, que garante integridade de acesso, fixando o endereço IP ao domínio da aplicação no host da máquina, não deixando outros plugins maliciosos agirem no navegador, criptografia, entre outras. Realiza boa proteção, porém esse método acaba sendo intrusivo, pois obriga a instalação de um aplicativo na máquina, que de certa forma acaba impactando na performance do navegador e é limitado a determinados sistemas operacionais.*

O problema deste tipo de mecanismo é que ele acaba interrompendo a conexão com outros serviços online, pois o *Warsaw* inicia junto com o computador, desta forma, seu funcionamento não está restrito ao acesso aos *Internet Banking*[19], mas acaba impedindo a conexão em qualquer outro serviço que utilize a comunicação de IPs. Além disso, em alguns dispositivos, o programa apresenta falhas e travamento do sistema (HIGA, 2015).

Com isto, o fundamental, seria que se desenvolvessem novos programas, ou extensões, que funcionem restritamente ao acesso da loja virtual, desta forma, evitaria a comunicação com outros dispositivos apenas no momento em que o usuário estivesse realizando a compra.

[19] Serviço de banco através da internet, disponibilizado pelas agências bancárias em seus domínios eletrônicos.

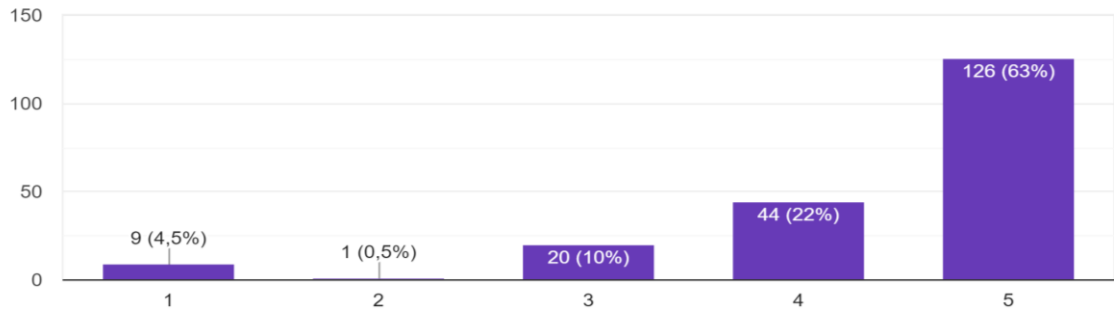
3 VERIFICAÇÃO DA PROPOSTA

Conforme as respostas do questionário aplicado, e com o que foi exposto no Capítulo 2 desta presente monografia, pudemos perceber, que é necessário que se projete novos mecanismos de segurança para o comércio eletrônico, de forma a aumentar a garantia de segurança neste meio de comércio.

Ao perguntar aos usuários, em questionário aplicado através de formulário eletrônico, sua opinião sobre a utilização dos mecanismos propostos, no caso, o uso de SMS, e de programas que evitem a conexão com outros dispositivos, a ser respondido em uma escala linear, onde **“1”** representa “péssimo” e **“5”** “ótimo”, obtiveram-se respostas favoráveis a aplicação de ambos os mecanismos.

Para a primeira proposta, pudemos perceber conforme os resultados que estão dispostos no gráfico 8, que 170 (85%) dos usuários se mostrou favorável[20] ao uso da confirmação da compra via SMS, enquanto somente 10 (5%) usuários foram contra o uso desse mecanismo.

Gráfico 8 - Uso de SMS com código para confirmar compra.

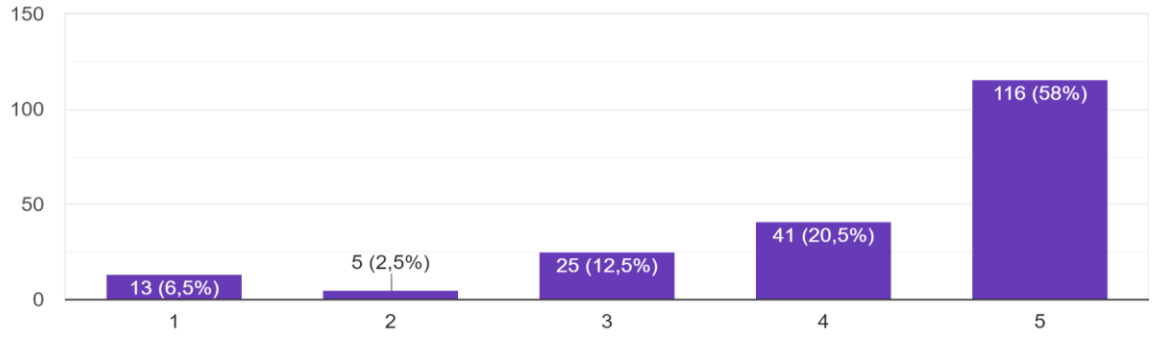


Fonte: Pesquisa elaborada pelo autor.

Já a segunda proposta, uso de programas para evitar a conexão com outros dispositivos no momento da compra, obteve um resultado onde 157 (78,5%) usuários se mostraram favoráveis, e 18 (9%) se mostraram desfavoráveis a seu uso, conforme podemos observar no gráfico 9. Desta forma, apesar de ainda ter uma grande maioria se posicionando a favor de tal mecanismo, o número de usuário que se mostrou contra aumentou consideravelmente.

[20]Nos gráficos de escala linear as respostas 1 e 2, foram interpretadas como não favorável; 3 como neutro; e 4 e 5 como favorável.

Gráfico 9 - Uso de programas que evitem a conexão com outros dispositivos.



Fonte: Pesquisa elaborada pelo autor.

O Banco Central Europeu *apud* Banco de Portugal (2013) divulgou através de um relatório realizado pelo Banco Central Europeu sobre fraudes com cartão, que, após a inclusão de novos mecanismos de segurança na União Europeia, incluindo o 3-D Secure, o número de fraudes que encontrava-se crescente até 2007 começou a cair anualmente. Conforme o relatório, do ano de 2007 até o ano de 2011 o número de fraudes a cartão de crédito caiu 7,6%, enquanto a renda obtida com as transações aumentou 10,3%.

Colaborando com o que foi mencionado, diz a CA Technologies (2018), desenvolvedora do 3-D Secure,

> *As soluções de segurança de pagamentos da CA Technologies ajudam as empresas de cartões a superar os obstáculos oferecendo autenticação automatizada para seus clientes. Essas soluções podem ajudá-las a obter maior sucesso ao evitar fraudes no comércio eletrônico, aumentar a receita, reduzir os custos operacionais dos cartões e melhorar a experiência geral de compras on-line dos clientes.*

Foi perguntado também, no questionário, aos usuários como eles viam a eficiência de tais medidas, e o resultado mostrou-se muito positivo, onde 170 (85%) dos usuários respondeu que as medidas podiam se mostrar eficazes, enquanto somente 3 (1,5%) respondeu que não seriam eficazes. Os outros 27 (13,5%) se posicionou de forma neutra quando a eficácia dessas medidas. Com isto, podemos

perceber que a maioria dos usuários tem uma expectativa positiva em relação a tais medidas, e acreditam, que elas possam surtir os efeitos esperados.

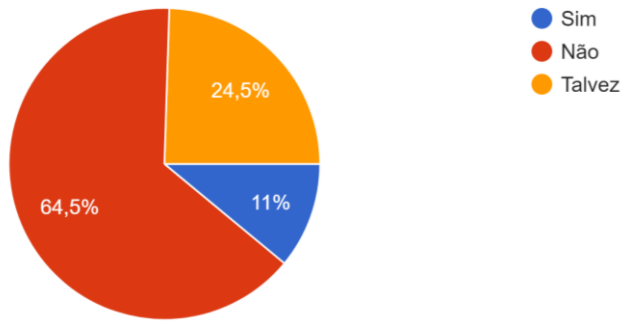
O uso do 3D-Secure, além de garantir uma maior segurança para o consumidor, traz benefícios também às empresas fornecedoras, pois com o seu uso, após a autenticação da compra com senha, mesmo com a realização de *chargebacks* pelos clientes quem arca com o prejuízo é o banco. Porém, ainda assim estas empresas são receosas quanto a implementação de tal mecanismo, visto que na época, o número de clientes que desistia da compra era muito alto, fazendo com que mesmo o fato de o *chargeback* recair sobre os bancos, a implementação de tal mecanismo não ser viável para as empresas (CANABARRO, 2014).

Já conforme a empresa Adyen (2018), o 3D-Secure vem sendo flexibilizado para o mercado, e algumas empresas que decidiram adotá-lo, já conseguem ver os resultados, é o caso do *Peixe Urbano*, conforme depoimento de seu CEO Alexander Tabor,

> *Desde o começo deste ano criamos regras flexíveis para o uso do 3D Secure. O resultado é impressionante: desde então, já recuperamos R$ 23 milhões. Vemos esta ferramenta como uma maneira de aumentar nosso faturamento com transações de risco que antes seriam declinadas, enquanto garantimos que os clientes verdadeiros não sejam interrompidos.*

Para corroborar isso, foi perguntado no questionário se as medidas propostas fariam com que os usuários deixassem de utilizar o comércio eletrônico, e os resultados, dispostos no gráfico 10, mostram que existem pouca tendência em o consumidor deixar de realizar negociações pelo comércio eletrônico caso as medidas fossem implementadas. Somente 22 (11%) dos usuários falou que com essas medidas o comércio eletrônico se tornaria menos atrativo, enquanto 129 (64,5%) falou que essas mudanças não trariam esse efeito negativo. Isso demonstra um interesse do usuário em utilizar medidas que tornem o comércio eletrônico mais seguro.

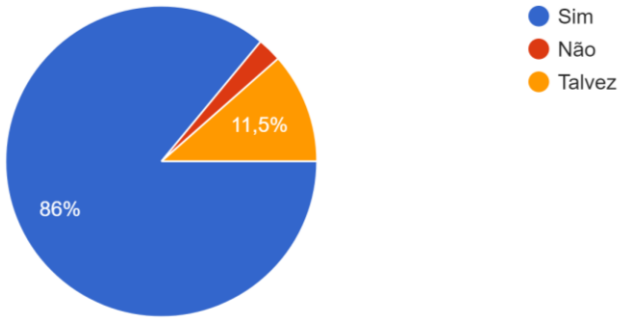
Gráfico 10 - Tendência a não comprar no comércio eletrônico caso as medidas propostas sejam implementadas.



Fonte: Pesquisa elaborada pelo autor.

Por fim, foi perguntado se estes mecanismos deveriam ser legalmente regulamentados, quanto a seu uso, sendo obrigatória sua aplicação a todas as lojas virtuais, e também a aderência dos usuários a eles. Como podemos ver no gráfico 11, apenas 5 (2,5%) pessoas acreditam que estes mecanismos não deveriam possuir previsão legal, enquanto 172 (86%) afirma que sim, deve existir uma regulamentação destes mecanismos.

Gráfico 11 - Deveriam estes mecanismos ter previsão legal?



Fonte: Pesquisa elaborada pelo autor.

Ressalta-se que a atual regulamentação do comércio eletrônico, Decreto-Lei 7.962/13, prevê o uso de mecanismos de segurança eficazes para o tratamento de dados dos clientes somente quando já estão em posse desses. Conforme podemos perceber pelo que diz Antonio Rulli Neto, Marcelo Adelino Asamura Azevedo e Renato Asamura Azevedo (2012),

> Os dados pessoais são preservados por disposição constitucional. Sua recepção, guarda e proteção são responsabilidade do sítio fornecedor. Ainda que dependa de outros para o armazenamento, a partir do momento que coleta os dados passa a ser responsável por sua guarda perante o consumidor. Difundir as informações significa permitir que os dados sejam utilizados por terceiros, não relacionados ao negócio e sem a devida autorização.

Porém, é necessário que essa proteção se estenda também a obtenção dos dados, ou antes da coleta como destacam os autores, onde na maioria dos casos, aqueles intencionados a aplicar as fraudes conseguem acesso eles.

Desta forma, observa-se uma necessidade no desenvolvimento de novos mecanismos de segurança para o comércio eletrônico, de forma a deixá-lo mais seguro tanto para o consumidor, como para o próprio fornecedor ou prestados do serviço. Por isto, estes mecanismos que foram apresentados podem ser bastante eficazes, pois além de prover uma maior segurança para os consumidores, podem também fazer com que as lojas passem a alcançar também potenciais consumidores que antes não tinham suas compras liberadas por conta de se localizarem em locais de risco, e dando a estes, a possibilidade de poder utilizar o comércio eletrônico.

CONCLUSÃO

Após realizadas as pesquisas, e elaborada esta monografia, com base no que nela fora exposto, pôde-se concluir que de fato existe uma relação entre a busca por uma maior liberdade no comércio eletrônico.

O aumento da liberdade observou-se pelo fato de os usuários terem como principal motivo para realizar as compras menor preço, e maior praticidade, os quais, impulsionam o mercado eletrônico e geram um aumento gradativo deste mercado anualmente.

Por outro lado, é possível verificar uma diminuição de segurança, quando verifica-se que o número de fraudes aplicadas no comércio eletrônico, ao longo dos últimos anos, vem aumentando em maior proporção que o próprio mercado eletrônico.

Este fato está relacionado não só com os avanços tecnológicos, que proporcionam aos aplicadores de golpes mais meios para aplicá-los, como principalmente ao não conhecimento, ou uso, dos usuários de mecanismos de segurança, como *antispywares* e *firewall*, o que torna a compra online sujeita a uma maior incidência de fraudes.

Por conta disso, faz-se necessário que novos mecanismos, que sejam mais incisivos quanto a seu uso, não ficando somente em função da prática do consumidor, sejam implementados no comércio eletrônico brasileiro, mecanismos estes, que já demonstraram resultados positivos quando implementados em outras nações e empresas, por exemplo, o 3D-Secure nesse trabalho proposto.

Através de pesquisa, na forma de um questionário, aplicada por meio de formulário eletrônico, notou-se que o desenvolvimento e implementação de novos mecanismos de segurança ao comércio eletrônico, embora ofereçam uma diminuição da liberdade aos consumidores, isso porque, tornam a compra menos cômoda e prática, apresentou grande aceitação popular.

É uma prática que traz benefícios não só para o consumidor, mas também para as empresas que possuem lojas virtuais, pois com a diminuição de fraudes, a quantidade de chargebacks também tende a diminuir, e com isso, estas passam a ter um menor prejuízo com a prática de fraudes, enquanto os consumidores, são poupados da dor de cabeça de ter de resolver o problema.

Esta troca pode ser justificada através da concepção de Estado de Hobbes e Rousseau, onde, através de um contrato social, os cidadãos abrem mão de suas liberdades individuais em troca da segurança do coletivo.

Deste modo, embora já existam legislações que discorram sobre a proteção de dados na internet, a inclusão através de previsão legal destes mecanismos é fundamental para que se possa dar mais segurança ao comércio eletrônico, favorecendo seu crescimento saudável.

REFERÊNCIAS

1. ACTIVEWEB. **O que é um certificado SSL?** 2018. Disponível em: <https://www.rapidssl.com.br/certificado-ssl>. Acesso em: 30 out. 2018.

2. ADYEN. **3D Secure: uma nova visão**. São Paulo, 2018.

3. AGILITY NETWORKS. **Segurança antifraude**. 2016. Disponível em: <http://www.agilitynetworks.com.br/blogdaagility/seguranca-antifraude/>. Acesso em: 20 out. 2018.

4. ALBERTIN, Alberto Luiz; MOURA, Rosa Maria de. Comércio eletrônico: seus aspectos de segurança e privacidade. **RAE-Revista de Administração de Empresas**, vol. 38, n. 2, 1998. Disponível em: <http://www.fgv.br/rae/artigos/revista-rae-vol-38-num-2-ano-1998-nid-46121/>. Acesso em: 08 nov. 2018.

5. ALECRIM, Emerson. **O que é ransomware?** 2016. Disponível em: <https://www.infowester.com/ransomware.php>. Acesso em: 28 jun. 2018.

6. ALMEIDA, R. E.S.; BRENDLE, V.; SPÍNOLA, N. D. **E-COMMERCE: Evolução, processo de compra e o desafio da entrega. Revista de desenvolvimento econômico**, SALVADOR, BA, v. 16, n. 29, p. 138-149, dez. 2014. Disponível em <https://revistas.unifacs.br/index.php/rde/article/view/3251/2342>. Acesso em: 25 out. 2018.

7. ALVES, Leandro de Carvalho; GONÇALVES, Fabiolla Valeria; MOIZINHO, Luzelia Calegari Santos. O custo da fraude: uma análise de um eCommerce brasileiro. **XX Congresso Brasileiro de Custos,** Uberlândia, 2013. Disponível em: <https://anaiscbc.emnuvens.com.br/anais/article/download/51/51>. Acesso em: 11 nov. 2018.

8. AQUINO JÚNIOR, Geraldo Frazão de. **Contratos eletrônicos: A boa fé objetiva e a Autonomia da Vontade.** Curitiba: Juruá, 2012. 113 p

9. ARROYO, C.S et al. Uma análise das preferências de consumidores no comércio eletrônico. **Revista FACEF PESQUISA**. v.9, n.1.2006. Disponível em: <http://periodicos.unifacef.com.br/index.php/facefpesquisa/article/view/62>. Acesso em: 04 nov. 2018.

10. AVAST, **Malware & Anti-malware**. 2018. Disponível em: <https://www.avast.com/pt-br/c-malware>. Acesso em: 17 jun. 2017.

11. AVAST, **Spyware**. 2018. Disponível em: <https://www.avast.com/pt-br/c-spyware>. Acesso em: 17 jun. 2017.

12. AVAST, **Trojan**. 2018. Disponível em: <https://www.avast.com/pt-br/c-trojan>. Acesso em: 17 jun. 2017.

13. AVAST. **Rootkit.** 2018. Disponível em: <https://www.avast.com/pt-br/c-rootkit>. Acesso em: 28 jun. 2018.

14. AVAST. **Ransomware**. 2018. Disponível em: <https://www.avast.com/pt-br/c-ransomware>. Acesso em: 28 jun. 2018.

15. BANCO DE PORTUGAL. **Relatório do BCE mostra uma queda da fraude com cartões**. 2013. Disponível em <https://www.bportugal.pt/comunicado/relatorio-do-bce-mostra-uma-queda-da-fraude-com-cartoes>. Acesso em: 04 nov. 2018.

16. BERALDI, Fidel. **Atualização dinâmica de modelo de regrassão logística binária para detecção de fraudes em transações eletrônicas com cartão de crédito.**2014. 156 f. Dissertação (Mestrado) - Curso de Ciência da Computação, Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2014. Disponível em: <http://www.teses.usp.br/teses/disponiveis/45/45134/tde-05022015-232801/en.php>. Acesso em: 12 nov. 2018.

17. BRASIL. **Decreto Lei nº 7962, de 15 de março de 2013**. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Brasília, 15 mar. 2013. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm>. Acesso em: 05 jun. 2017.

18. BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, 23 abr. 2014. Disponível em: < http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm>. Acesso em 26 jun. 2017.

19. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, 14 ago. 2018. Disponível em:< http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 20 set. 2018.

20. BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, 11 set. 1990. Disponível em: < http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm>. Acesso em: 28 jun. 2017.

21. BREEDEN, Simon. **Segurança na Era Digital**. 2017. Disponível em: <https://ecommercenews.com.br/artigos/dicas-artigos/seguranca-na-era-digital/>. Acesso em: 06 nov. 2018.

22. CANABARRO, Tom. **Principais causas de fraude no E-commerce**. 2014. Disponível em: <https://blog.konduto.com/pt/2015/02/as-causas-da-fraude-parte-1/>. Acesso em: 04 nov. 2018.

23. CANUT, Letícia. **Proteção do Consumidor no Comércio Eletrônico: Uma Questão de Inteligência Coletiva que Ultrapassa o Direito Tradicional**. Curitiba: Juruá Editora, 2007. p. 266.

24. CARICATTI, André Machado. **O Local do Crime no Ciberespaço**. In: BLUM, Renato M. S. Opice; BRUNO, Marcos Gomes da Silva; ABRUSIO, Juliana Canha. Manual de Direito Eletrônico e Internet. São Paulo: Lex Editora, 2006. Cap. 5, p. 65-77.

25. CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. In: Âmbito Jurídico, Rio Grande, XV, n. 99, abr 2012. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529>. Acesso em 16 jun. 2017.

26. CCM. **O que é um proxy?** 2018. Disponível em: <https://br.ccm.net/faq/9414-o-que-e-um-proxy>. Acesso em: 28 ago. 2018.

27. CISCO. **O que é um Firewall?** Disponível em: <https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html>. Acesso em: 03 nov. 2018.

28. CLEARSALE. **Mapa da Fraude 2018.** 2018. Disponível em: <https://d335luupugsy2.cloudfront.net/cms/files/29144/1524251746mapa-da-fraude-2018.pdf>. Acesso em: 15 out. 2018.

29. COELHO, Fábio Ulhoa. **Curso de direito comercial**. São Paulo: Saraiva, 2000. v. 3.

30. COELHO, Lidiane da Silveira; OLIVEIRA, Rafaela Carvalho; ALMÉRI, Tatiana Martins. O CRESCIMENTO DO E-COMMERCE E OS PROBLEMAS QUE O ACOMPANHAM: a identificação da oportunidade de melhoria em uma rede de comércio eletrônico na visão do cliente. **Revista de Administração do Unisal**, [S.l.], v. 3, n. 3, maio 2013. ISSN 1806-5961. Disponível em: <http://www.revista.unisal.br/sj/index.php/RevAdministracao/article/view/235>. Acesso em: 30 out. 2018.

31. CONSTANT, Benjamin. “De la liberté des anciens comparée a celle des modernes”, In : De la liberté chez les modernes. **Ecrits politiques**, Paris, 1980, p. 491 e seguintes.

32. CORREIA, Miguel Pupo. Comércio Electrónico: Forma e Segurança. In MONTEIRO, António Pinto (coord.). **As Telecomunicações e o Direito na Sociedade da Informação**. Coimbra : Instituto Jurídico da Comunicação, 1999. p. 223-258.

33. COUTO, Rute Isabel Esteves Ferreira. **COMÉRCIO E CONSUMO ELECTRÓNICO: ALGUMAS CONSIDERAÇÕES JURÍDICAS**. 2004. 166 f. Dissertação (Mestrado) - Curso de Direito, Universidade Católica Portuguesa, Faculdade de Direito, Porto, 2004. p.35. Disponível em: <https://bibliotecadigital.ipb.pt/bitstream/10198/6146/1/RuteCouto_TeseMESTRADO_ComércioConsumoElectrónico.pdf>. Acesso em: 14 jun. 2017.

34. CROCCO, Luciano. et al. **Marketing: perspectivas e tendências**. São Paulo, Saraiva, 2010.

35. DINIZ, L.L et al. **O Comércio Eletrônico como Ferramenta Estratégica de Vendas para Empresas**. III Encontro Científico e Simpósio de Educação Unisalesiano, Lins, p. 1- 13, out. 2011. Disponível em: <http://www.unisalesiano.edu.br/simposio2011/publicado/artigo0093.pdf>. Acesso em: 20 jun. 2018.

36. DIZER o Direito. **Lei 13.709/2018: Lei Geral de Proteção de Dados Pessoais**. Disponível em: <https://www.dizerodireito.com.br/2018/08/lei-137092018-lei-geral-de-protecao-de.html>. Acesso em: 09 set. 2018.

37. EBIT. **Webshoppers**. 38 ed., 2018. Disponível em: <https://www.ebit.com.br/webshoppers>. Acesso em: 25 set. 2018.

38. EBIT. **Webshoppers**. 37 ed., 2017. Disponível em: <https://www.ebit.com.br/webshoppers>. Acesso em: 30 set. 2018.

39. E-COMMERCE BRASIL. **Pesquisa aponta que quase um terço dos consumidores brasileiros on-line já sofreu fraudes**. 2016. Disponível em: <https://www.ecommercebrasil.com.br/noticias/pesquisa-aponta-que-quase-um-terco-dos-consumidores-brasileiros-on-line-ja-sofreu-fraudes/>. Acesso em 08 nov. 2018.

40. FAGUNDES, Eduardo. **O QUE É E-COMMERCE?** 2011. Disponível em: <http://efagundes.com/artigos/o-que-e-e-commerce/>. Acesso em: 12 jun. 2018.

41. FAGUNDES, Eduardo. **Novas Tecnologias e Práticas para a Segurança da Informação**. 2014. Disponível em: <http://efagundes.com/artigos/novas-tecnologias-e-praticas-para-a-seguranca-da-informacao/>. Acesso em: 05. nov. 2018.

42. FELICIANO, Guilherme Guimarães. Informática e criminalidade. Parte I: lineamentos e definições**. Boletim do Instituto Manoel Pedro Pimente**l, São Paulo, v. 13, n. 2, p. 35-45, set. 2000. p. 42.

43. FERREIRA, G. A fraude no comércio eletrônico. **Revista E-Commerce Brasil**, São Paulo, v. 32, p. 48-49, abr. 2016. Disponível em: <https://www.ecommercebrasil.com.br/revista/a-revolucao-plus-size-comeca-na-internet>. Acesso em: 19 ago. 2018.

44. GIMENES, Emanuel Alberto Sperandio Garcia. Crimes virtuais. **Revista de Doutrina da 4ª Região**, Porto Alegre, n. 55, ago. 2013. Disponível em: <http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html> Acesso em: 17 nov. 2017.

45. GOBERTO, M. **Desvantagens do Comércio Eletrônico**, 2012. Disponível em: <https://ecommercenews.com.br/artigos/cases/desvantagens-do-comercio-eletronico/>. Acesso em: 30 jun. 2018.

46. GUASTI, P. **E-Commerce: Um negócio de sucesso**. 2010. Disponível em: <https://empresa.ebit.com.br/artigo-livro-2010.asp>. Acesso em: 25 out. 2018.

47. HAUTSCH, O. **Como funciona o Firewall?** 2010. Disponível em: <http://www.tecmundo.com.br/seguranca/3329-como-funciona-o-firewall-.htm>. Acesso em: 28 ago. 2018.

48. HIGA, Paulo. **O plugin de segurança que os bancos usam está causando problemas de acesso a alguns sites**. 2015. Disponível em: <https://tecnoblog.net/176402/plugin-bancos-warsaw-ipv6-bloqueio/>. Acesso em: 04 nov. 2018.

49. HOBBES, Thomas. **O Leviatã: ou Matéria, Forma e Poder de Um Estado Eclesiástico e Civil.** São Paulo: Martin Claret, 2014. Tradução de: Rosina D'Angina.

50. KASPERSKY. **O que é antivírus na nuvem?** 2018. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/cloud-antivirus>. Acesso em: 02 nov. 2018.

51. KASPERSKY. **Como o antispyware oferece a melhor defesa para seu computador**. 2018. Disponível em: <https://www.kaspersky.com.br/resource-center/preemptive-safety/antispyware-provides-best-computer-defense>. Acesso em: 02. nov. 2018.

52. KASPERSKY. **O que são Rootkits e como Enfrentá-los**. 2013. Disponível em: <https://www.kaspersky.com.br/blog/o-que-sao-rootkits-e-como-enfrenta-los/769/>. Acesso em: 28 jun. 2018.

53. KASPERSKY. **O que é adware?** 2018. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/adware>. Acesso em: 28 jun. 2018.

54. KLEE, Antonia Espíndola Longoni. Comércio Eletrônico. São Paulo: **Revista dos Tribunais**, 2014.

55. LEMONNIER, Jonathan. **O que é adware e como se livrar dele?** 2016. Disponível em: <https://www.avg.com/pt/signal/what-is-adware>. Acesso em: 28 jun. 2018.

56. LEONI, Bruno. ***Liberdade e Lei***. São Paulo: Instituto Ludwig Von Mises Brasil, 2010. p. 67. Tradução de: Rosélis Maria Pereira e Diana Nogueira.

57. LOPEZ, Bianca. **Consumidores do e-commerce no Brasil: perfil e comportamento**. 2018. Disponível em: <https://www.pagbrasil.com/pt-br/noticias/consumidores-de-e-commerce-brasil/>. Acesso em: 07 nov. 2018.

58. LÓPEZ, Martínez. SISTEMAS DE PAGO SEGURO. SEGURIDAD EN EL COMÉRCIO ELECTRÓNICO. **Revista de Estudios Empresaliales,** Jaén, 2009, 63-76 p. Disponível em: <https://revistaselectronicas.ujaen.es/index.php/REE/article/view/359/322>. Acesso em: 20 out. 2018.

59. LUDMER, Eduardo. **Comércio Eletrônico no Brasil: Quatro anos do Decreto 7962/2013**. 2017. Disponível em:

<https://www.thomsonreuters.com.br/pt/juridico/blog/comercio-eletronico-no-brasil-quatro-anos-do-decreto-7962-2013.html>. Acesso em: 09 set. 2018.

60. MACAREZ, Nicolas ; LESLÉ, François. **Comércio Electrónico**. Mem Martins : Editorial Inquérito, 2002. p. 20-22.

61. MARQUES, Ana Margarida ; ANJOS, Mafalda ; VAZ, Sónia Queiroz. **101 Perguntas e Respostas do Direito da Internet e da Informática**. Centro Atlântico, 2002. p. 5.

62. MARQUES, Cláudia Lima. **Confiança no comércio eletrônico e a proteção do consumidor: um estudo dos negócios jurídicos de consumo no comércio eletrônico.** São Paulo: Revista dos Tribunais, 2004.

63. MARTINS, Guilherme Magalhães. **Contratos eletrônicos de consumo**. 3. ed. São Paulo: Atlas, 2016. 270-274 p.

64. MICROSOFT. **Golpes de Phishing**. Disponível em: <https://www.microsoft.com/pt-br/security/online-privacy/phishing-faq.aspx>. Acesso em: 17 jun. 2017.

65. MICROSOFT. **Microsoft Secure**. Disponível em: <https://www.microsoft.com/pt-br/security/threat-protection>. Acesso em: 20 out. 2018.

66. MICROSOFT. **O que é software antivírus?** Disponível em: <https://www.microsoft.com/pt-br/security/resources/antivirus-whatis.aspx>. Acesso em: 03 nov. 2018.

67. MICROSOFT. **O que é software antispyware?** Disponível em: <https://www.microsoft.com/pt-br/security/resources/antispyware-whatis.aspx>. Acesso em: 02 nov. 2018

68. MIRANDA, C. M. C.; ARRUDA, D. M. de O. E-produtos e variáveis comportamentais determinantes de compra no varejo virtual: um estudo com consumidores brasileiros. **REAd–** 37. ed., v. 10, n. 1, janeiro – fevereiro, 2004. Disponível em: <https://seer.ufrgs.br/read/article/view/42552/26943>. Acesso em: 31 out. 2018.

69. MOREIRA, Eric. **Criptografia, a chave da sua segurança.** 2018. Disponível em: <https://ecommercenews.com.br/artigos/dicas-artigos/criptografia-a-chave-da-sua-seguranca/>. Acesso em: 14 nov. 2018.

70. NASCIMENTO, A.R.; SILVA, B.R.; SANTOS, G.G. **E-commerce: O Melhor Caminho no Mercado Atual**. 2009. Monografia (Curso de Administração) - Centro Universitário Eurípides de Marília, Marília, 2009. p. 23-24. Disponível em: <http://aberto.univem.edu.br/bitstream/handle/11077/496/E-commerce%3A%20O%20Melhor%20Caminho%20no%20Mercado%20Atual.pdf?sequ>. Acesso em: 20 out. 2018.

71. NETO, Antonio Rulli; AZEVEDO, Marcelo Adelino Asamura; AZEVEDO, Renato Asamura. **Regulamentação do comércio eletrônico no Brasil e um**

contexto de tutela à pessoa na Sociedade da Informação. 2012. Disponível em: <https://por-leitores.jusbrasil.com.br/noticias/100491167/regulamentacao-do-comercio-eletronico-no-brasil-e-um-contexto-de-tutela-a-pessoa-na-sociedade-da-informacao>. Acesso em: 12 nov. 2018.

72. NORTON. **O que é um vírus de computador?** 2018. Disponível em: <https://br.norton.com/internetsecurity-malware-what-is-a-computer-virus.html>. Acesso em: 20 jun. 2018.

73. OLIVEIRA, Carlos Eduardo Elias de. **Aspectos Principais da Lei nº 12.965, de 2014, o Marco Civil da Internet: subsídios à comunidade jurídica**. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/ Senado, abr./2014 (Texto para Discussão nº 148). Disponível em: www.senado.leg.br/estudos. Acesso em 17 de junho de 2017.

74. PACHECO, Phillipe de Souza. **Comércio Eletrônico: Conflitos judiciais decorrentes de relações de consumo virtual**. 2015. Disponível em: <https://juridicocerto.com/p/phillipepacheco/artigos/comercio-eletronico-conflitos-judiciais-decorrentes-de-relacoes-de-consumo-virtual-1352>. Acesso em: 16 jun. 2017.

75. PANDA SECURITY. **Worms**. 2018. Disponível em: <https://www.pandasecurity.com/brazil/homeusers/security-info/classic-malware/worm/>. Acesso em: 30 jun. 2018.

76. PAYZEN. **3D Secure.** 2018. Disponível em: <https://payzen.com.br/seguranca/3d-secure/>. Acesso em: 20 out. 2018.

77. PEREIRA, Alexandre Dias. **Comércio electrónico na sociedade da informação: da segurança técnica à confiança jurídica**. Coimbra: Almedina, 1999. p. 15.

78. PULIDO, Carlos Bernal. **O conceito de liberdade na teoria política de Norberto Bobbio**. PANÓPTICA - Direito, Sociedade e Cultura, [S.l.], v. 4, n. 2, p. 50, jul. 2009. ISSN 1980-7775. Disponível em: <http://www.panoptica.org/seer/index.php/op/article/view/Op_4.2_2009_48-71>. Acesso em: 12 Jun. 2017.

79. PWC. **Total Retail 2016 – A revolução que os consumidores almejam, com a execução que os conquista.** 2016. Disponível em: <https://www.pwc.com.br/pt/setores-de-atividade/varejo-e-consumo/assets/2016/total_retail_16_brasil.pdf>. Acesso em: 30 set. 2018.

80. REALE, Miguel. **Teoria tridimensional do direito**. 5. ed. São Paulo : Saraiva, 1994.

81. REALPROTECT. **4 tipos de malware que você deve ficar atento**. 2015. Disponível em: < https://realprotect.net/blog/4-tipos-de-malware-que-voce-deve-ficar-atento>. Acesso em: 20 jun. 2018.

82. REEDY, Joel; Schullo, Shauna. **Marketing eletrônico: integrando recursos eletrônicos no processo de marketing**. São Paulo, Thomson Learning, 2007.

83. REIS, Wanderlei José dos. DELITOS CIBERNÉTICOS: IMPLICAÇÕES DA LEI Nº 12.737/12. **Connection Line**, São Paulo, v. 13, p.127-134, jun. 2015. Semestral. Disponível em: <http://www.periodicos.univag.com.br/index.php/CONNECTIONLINE/article/view/251/491>. Acesso em: 17 jun. 2017.

84. RESENDE, Dilma A. Certificação Digital. **Revista Jurídica UNIGRAN**, Dourados, MS, v. 11, n. 22, p. 111-121, dez.2009. Disponível em: <http://www.unigran.br/revista_juridica/ed_anteriores/22/artigos/artigo09.pdf>. Acesso em: 30 out. 2018

85. RIBEIRO, O.G et al. DIGITAL CERTIFICATION ON THE ICP-BRASIL. **Revista Tékhne E Lógos**, São Paulo, v.2, n.2, p.57-72, fev. 2011. Disponível em: <http://www.fatecbt.edu.br/seer/index.php/tl/article/view/105/64>. Acesso em: 16 out. 2018.

86. RODRIGUES, Carlos Alexandre. Da desnecessidade de assinatura para a validade do contrato efetivado via Internet. **Revista dos Tribunais**, São Paulo, v. 784, p. 83-95, fev. 2001.

87. ROLLO, A. L. M. O Consumidor e as Compras através da Internet. **Universo Jurídico**, Juiz de Fora, p. 1-1, jul. 2008.

88. ROUSSEAU, Jean-Jacques. **O Contrato Social**. Porto Alegre: L&PM, 2016. p. 34. Apresentação de João Carlos Brum Torres; Tradução de: Paulo Neves.

89. ROVER, Aires José. **Direito e Informática**. Barueri: Manole, 2004.

90. SANTANDER. **Token Santander**. 2018. Disponível em: <https://www.santander.com.br/portal/wps/script/templates/GCMRequest.do?page=8488>. Acesso em: 04 nov. 2018.

91. SILVA, Aidam Santos. **Acesso à Justiça no comércio eletrônico**. 2015. Disponível em: <https://aidamjuris.jusbrasil.com.br/artigos/194871718/acesso-a-justica-no-comercio-eletronico>. Acesso em: 26 out. 2018.

92. SILVA, Miguel Mira da ;et al. **Comércio Electrónico na Internet**. 2ª ed. actualizada. Lidel Edições Técnicas, 2003. p. 2

93. SILVA, Paulo Quintiliano da. **Crimes Cibernéticos e seus Efeitos Internacionais.** 2006. Disponível em: <http://icofcs.org/2006/ICoFCS2006-pp02.pdf>. Acesso em: 18 jun. 2017.

94. SILVA NETO, Abdo Dias da. C**ontratos eletrônicos e a aplicação da legislação moderna**. In: Âmbito Jurídico, Rio Grande, XI, n. 60, dez 2008. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=5365>. Acesso em jun 2017.

95. SMITH, et al. Case studies of cybercrime and their impact on marketing activity and shareholder value. **Academy of Marketing Studies Journal**, v. 15, n. 2, 2011.

96. STJ, **Comércio eletrônico cresce de forma exponencial e gera demandas no Judiciário**. 2018. Disponível em: <http://www.stj.jus.br/sites/STJ/default/pt_BR/Comunica%C3%A7%C3%A3o/noticias/Not%C3%ADcias/Com%C3%A9rcio-eletr%C3%B4nico-cresce-de-forma-exponencial-e-gera-demandas-no-Judici%C3%A1rio>. Acesso em: 20 out. 2018.

97. TORRES, Gonzalo. **O que é um vírus de computador?**, 2019. Disponível em: < https://www.avg.com/pt/signal/what-is-a-computer-virus>. Acesso em: 20 jun. 2018.

98. VISA. **O que é o Verified by Visa**. 2018. Disponível em: <https://www.visa.com.br/pague-com-visa/tecnologias-em-destaque/verified-by-visa-para-consumidores.html>. Acesso em: 05 nov. 2018.

99. VOLPI, Marlon Marcelo. Um Contrato Social para a Internet. In: BLUM, Renato M. S. Opice; BRUNO, Marcos Gomes da Silva; ABRUSIO, Juliana Canha. **Manual de Direito Eletrônico e Internet**. São Paulo: Lex Editora, 2006. Cap. 4, p. 49-61.

APÊNDICE 1

A troca da segurança pela liberdade na Internet: Uma análise das consequências do comércio eletrônico.

Formulário com a finalidade de obter dados qualitativos para a produção de monografia na área de direito eletrônico.

*Obrigatório

1. **Idade** *

2. **Escolaridade** *
Marcar apenas uma oval.
- ◯ Ensino Fundamental incompleto
- ◯ Ensino Fundamental completo
- ◯ Ensino Médio incompleto
- ◯ Ensino Médio completo
- ◯ Ensino Superior incompleto
- ◯ Ensino Superior completo

3. **Você utiliza a internet para realizar compras?** *
Marcar apenas uma oval.
- ◯ Nunca
- ◯ Raramente
- ◯ Às vezes
- ◯ Quase sempre
- ◯ Sempre

4. **Quais motivos levam você a realizar compras via internet?** *
Marque todas que se aplicam.
- ☐ Maior variedade de opções
- ☐ Menores preços
- ☐ Praticidade
- ☐ Outro:

5. **Você já foi vítima de alguma fraude na internet?** *
Marque todas que se aplicam.

- [ ] Roubo de dados (CPF, Cartão de crédito/débito, conta bancária, etc)
- [ ] Não entrega do produto
- [ ] Compras no seu nome
- [ ] Valor cobrado diferente do apresentado na hora da compra
- [ ] Nunca fui vítima de fraudes na internet
- [ ] Outro: _____

6. **Quais destes mecanismos de segurança para compra na internet você usa?** *
Marque todas que se aplicam.

- [ ] Protocolo de segurança "https"
- [ ] Anti-vírus
- [ ] Antispyware
- [ ] Sites de reputação das lojas virtuais (por exemplo, eBit).
- [ ] Comentários de outros compradores sobre o site em que está realizando a compra.
- [ ] Não conheço/utilizo
- [ ] Outro: _____

Propostas de alternativas para a diminuição na incidência de crimes no comércio eletrônicos.

7. **Atualmente você se sente seguro ao realizar compras na internet?** *
Marcar apenas uma oval.

	1	2	3	4	5	
Não	◯	◯	◯	◯	◯	Sim

8. **O que você acharia de receber um SMS (enviado a número de telefone cadastrado na agência do cartão de crédito/débito) com um código para confirmar sua compra?** *
Marcar apenas uma oval.

	1	2	3	4	5	
Péssimo	◯	◯	◯	◯	◯	Ótimo

9. **Você utilizaria programas que evitam a conexão de seu computador a outro durante as compras online, diminuindo assim, o risco do roubo de seus dados?** *
Marcar apenas uma oval.

	1	2	3	4	5	
Péssimo	◯	◯	◯	◯	◯	Ótimo

10. Essas etapas a mais durante a compra, tornariam ela menos atrativa para você? *
Marcar apenas uma oval.

- Sim
- Não
- Talvez

11. **Você acha que é necessário desenvolver novos mecanismos de segurança para o comércio eletrônico, como os apresentados?** *
Marcar apenas uma oval.

- Sim
- Não
- Talvez

12. **Pela sua percepção, quão eficaz seriam essas medidas?** *
Marcar apenas uma oval.

	1	2	3	4	5	
Ineficaz						Muito eficaz

13. **Você acha que tais medidas deveriam ser legalmente regulamentadas?** *
Marcar apenas uma oval.

- Sim
- Não
- Talvez

14. **Comentários Gerais**

Powered by Google Forms